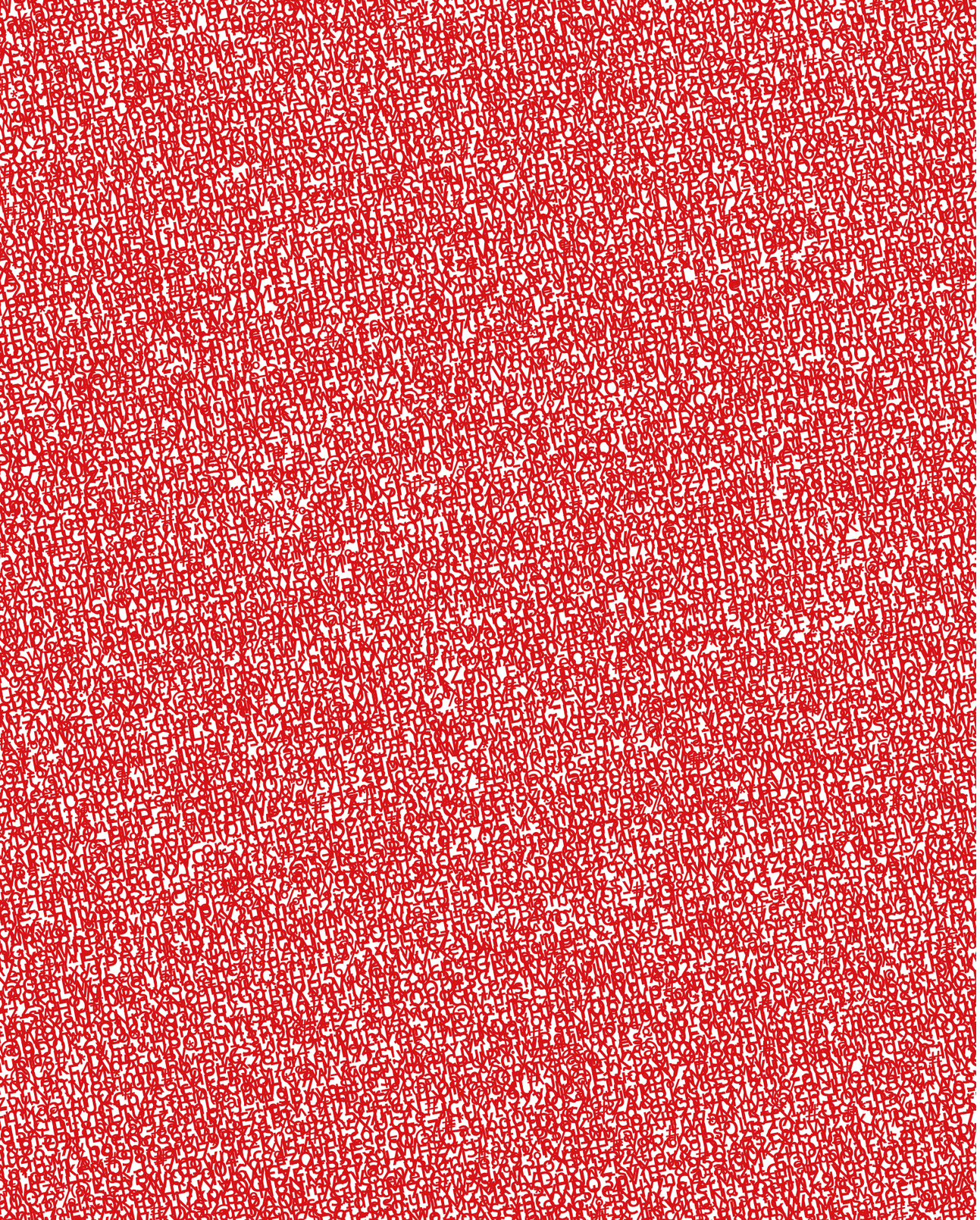
Joel Baumann / Jörn Lamla (Hg.)

PRIVACY ARENA

Kontroversen um Privatheit im digitalen Zeitalter

kassel university press

ewF0LmGIkXI
-kSpLIRyxo4gT^KqH4P
YqmU&iXFH_6#F9OpsB&
4rwm;&U
O0Z&T5YkquME
^-T6C
zVfUUOe*15C
g*lI2l2
zKcD#
RmVad%K0
iylo2Bs
L-C0eBsw~
$!Pr5*p
HOfU9nCDL28ce~
SGcenF-YYVuN2
xj62h3v
w3hC
S$W%aZ*0
_szRT1Z*kh3
QU7n8
3Sj@b^r0N4OH0E
GtxT*-K4ZImPXDFWB
Ma_gx
M-FZ^wg74D8b
t!MsesWxOX
dN0Eg
3dSoVZ
c!kp!0MD43PZ4
V^!aB&*W1K
Zey20gWzA5KbbGO~
gqziIL
ACI4X~*9XO
qpG
RKeX#
~pH
G5#



Joel Baumann / Jörn Lamla (Hg.)

PRI-VACY ARENA

Kontroversen um Privatheit im digitalen Zeitalter

Das dieser Publikation zugrundeliegende Vorhaben wurde mit Mitteln des Bundesministeriums für Bildung und Forschung unter dem Förderkennzeichen 16KIS0096K gefördert. Die Verantwortung für den Inhalt der Veröffentlichung liegt bei den Autoren.

Ein-leitung

von Joel Baumann, Jörn Lamla

01

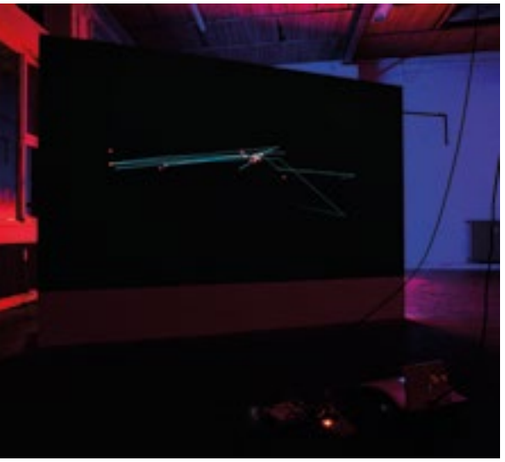
Dem vorliegenden Band liegen Untersuchungen zu den Kontroversen um Privatheit im digitalen Zeitalter zugrunde, die aus der Kooperation dreier Disziplinen – Soziologie, Rechtswissenschaft und Ethik/Philosophie – mit dem im Studiengang Visuelle Kommunikation verankerten Fachgebiet Neue Medien der Kunsthochschule Kassel hervorgegangen sind. Neben den beiden Herausgebern aus den Bereichen Kunst bzw. Soziologie und den Autor*innen der verschiedenen Beiträge waren daran Regina Ammicht Quinn, Jessica Heesen (beide Tübingen, Ethik/Philosophie) und Alexander Roßnagel (Kassel, Recht) sowie Carsten Ochs (Kassel, Soziologie) als weitere Antragsteller*innen beteiligt.

Die Zusammenarbeit mündete in Formen einer forschenden Verschränkung von Kunst und Wissenschaft, deren Ergebnisse in Gestalt einer Website (privacy-arena.net) und einer Kunstausstellung der Band vorstellen und um ein eigenes Format ergänzen will.

Wie kam es aber überhaupt zu dieser Kollaboration und warum ist sie folgerichtig? Dies wollen wir hier einleitend erläutern.

Ausgangspunkt des Projektes war die Exploration einer kartografischen Herangehensweise an das Thema Privatheit. Sinn und Zweck der Methode ist es, der Krise der Privatheit im digitalen Zeitalter gerade nicht durch den Rückgriff auf scheinbar objektive, unbestreitbare Tatsachen wissenschaftlich Herr zu werden, sondern vielmehr die tiefgreifende Verunsicherung und den umstrittenen Charakter dieser facettenreichen Thematik ernst zu nehmen. Gleichwohl

sollte auch nicht der gegenteilige Schluss gezogen und Privatheit als leerer Signifikant reiner Machtkämpfe oder gänzlich kontingenter politischer Positionierungen verstanden werden. Vielmehr steckt in der kartografischen Methode der Anspruch, beides zu sein: wissenschaftlich stringente



Aufzeichnung einer konflikthaften Materie und politische Artikulationshilfe angesichts neuer Verunsicherungen durch die Digitalisierung. Schon das zugrunde gelegte Konzept der Privacy-Arena deutet an, dass in dieser Arena eine Pluralität von Praktiken, Haltungen und Positionen versammelt ist, die allesamt um Deutungshoheit und/oder Durchsetzung ringen, dabei aber ungleiche Voraussetzungen und Chancen haben, Gehör zu finden. Ziel ist es, durch nachvollziehbare Rekonstruktionen mittels kartografischer

Beschreibungen eine Art Navigationshilfe für die an Fragen der Privatheit Interessierten zu schaffen. Das Projekt hat damit einen Bezug zur Praxis: Es begreift sich als eingebunden in einen Prozess öffentlicher Lösungssuche für die Probleme der Privatheit im digitalen Zeitalter. Unklar ist jedoch, wie die Wissenschaft einen solchen Anspruch realisieren kann, ohne ihre Identität und Integrität als Wissenschaft aufzugeben.

Wie lässt sich zwischen methodischer Strenge und öffentlichem Diskurs angemessen vermitteln?

Zu dieser Frage gibt es eine Reihe von Vorschlägen. So wird in der Soziologie im Anschluss an die Thesen von Michael Burawoy[1] diskutiert, ob sich das Fach über

1 Burawoy, Michael (2005): For Public Sociology. In: American Sociological Review 70 (1), S. 4 – 28.

die lange gepflegte kritische Distanz gegenüber seinem Untersuchungsbereich

hinaus stärker öffentlich engagieren sollte. Doch erscheint fragwürdig, ob die „organischen“ Bündnispartner der Zivilgesellschaft wirklich so leicht wie Burawoy nahe legt zu identifizieren sind, deren Stimmen die Öffentliche Soziologie dann nur noch reflektieren und verstärken müsste. Zu schnell mündet eine solche engagierte Beteiligung am sozialen Kampf in der Deprofessionalisierung als Wissenschaft.[2] Bescheidenere

2 Vgl. Lamla, Jörn (2014): Öffentlichkeit: Soziologie, Zeitdiagnose und Gesellschaftskritik. In: Lamla, J. et al. (Hrsg.): Handbuch der Soziologie. Konstanz: UVK, S. 491 – 505.

Ansätze stellen daher weniger auf inhaltliche Positionierung als Public Sociology ab, sondern betonen die Notwendigkeit, einfacher les- und sichtbar zu werden, etwa durch die Erarbeitung einer deutlich verbesserten visuellen Formensprache.[3] Doch

3 Beck, Gerald (2013): Sichtbare Soziologie. Visualisierung und soziologische Wissenschaftskommunikation in der Zweiten Moderne. Bielefeld: transkript.

auch damit wird sie ihrer Übersetzungs- und Vermittlungsaufgabe noch nicht gerecht, die nicht auf die Suche eines geeigneten

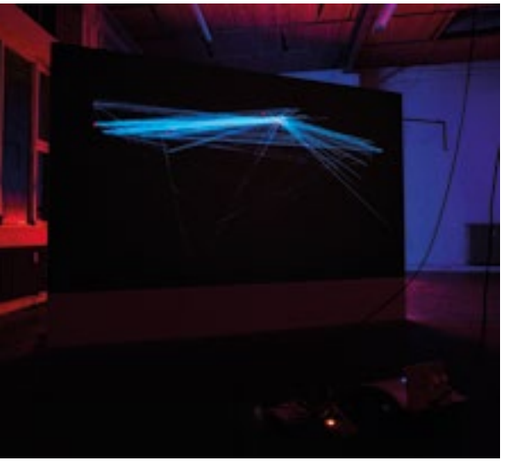
Mittelmaßes zwischen zu starker und zu geringer Komplexitätsreduktion verkürzt werden darf. Bei einem Untersuchungsgegenstand von öffentlichem Interesse geht es nicht nur darum, wie wissenschaftliche Botschaften verpackt werden oder für/gegen wen diese legitimerweise Partei ergreifen können. Vielmehr gilt es, der Öffentlichkeit als Teil der Untersuchung Möglichkeiten der (Selbst-)Reflexion und Neukonfiguration – m.a.W.: zum Lernen – zu eröffnen.

Genau dieser Ansatz wird in dem aus den Science & Technology Studies hervorgegangenen und an das pragmatistische Erbe John Deweys anschlussfähige Konzept des „Mapping of Controversies“ verfolgt.[4] Dabei

4 Vgl. Venturini, Tommaso (2010): Diving in magma. How to explore controversies with actor-network theory. In: Public Understanding of Science 19, S. 258 – 273; Venturini, Tommaso (2012): Building On Faults. How to represent controversies with digital methods. In: Public Understanding of Science 21, S. 796 – 812; Marres, Noortje/Moats, David (2015): Mapping Controversies with Social Media: The Case for Symmetry. In: Social Media and Society, 2, S. 1 – 17.

handelt es sich zunächst um experimentelle Navigationshilfen, die textbasiert sein

können, die aber auch digitale oder grafische Tools für eine interaktive Nutzung aufbereiteter oder im Netz verfügbarer Daten bereitstellen und damit den Nutzerinnen und Nutzern eine aktive Rolle bei der Generierung von Orientierungswissen zuweisen. Im Sinne von Atlanten werden Kontroversen



dabei nach spezifischen Fragen oder Themen gleich mehrfach kartografiert und dadurch differenziert dargestellt. Neben der aktiven Einbeziehung der Betrachterinnen und Betrachter gilt es hierbei zu reflektieren, inwiefern die Kartografie eine interessierte Öffentlichkeit präfiguriert und miterzeugt. So wie Europa flächenmäßig größer und Afrika sowie Südamerika kleiner auf Weltkarten in der Mercartor-Projektion erscheinen, gilt auch für die Kartografie einer Kontroverse, dass sie stets die Kontroverse performativ

miterzeugt und dass sie deshalb der Öffentlichkeit nicht neutral gegenübersteht.[5] Wenn

5 Venturini, Tommaso et al. (2015): Designing Controversies and their Publics. In: Design Issues, 31 (3), S. 74 – 87.

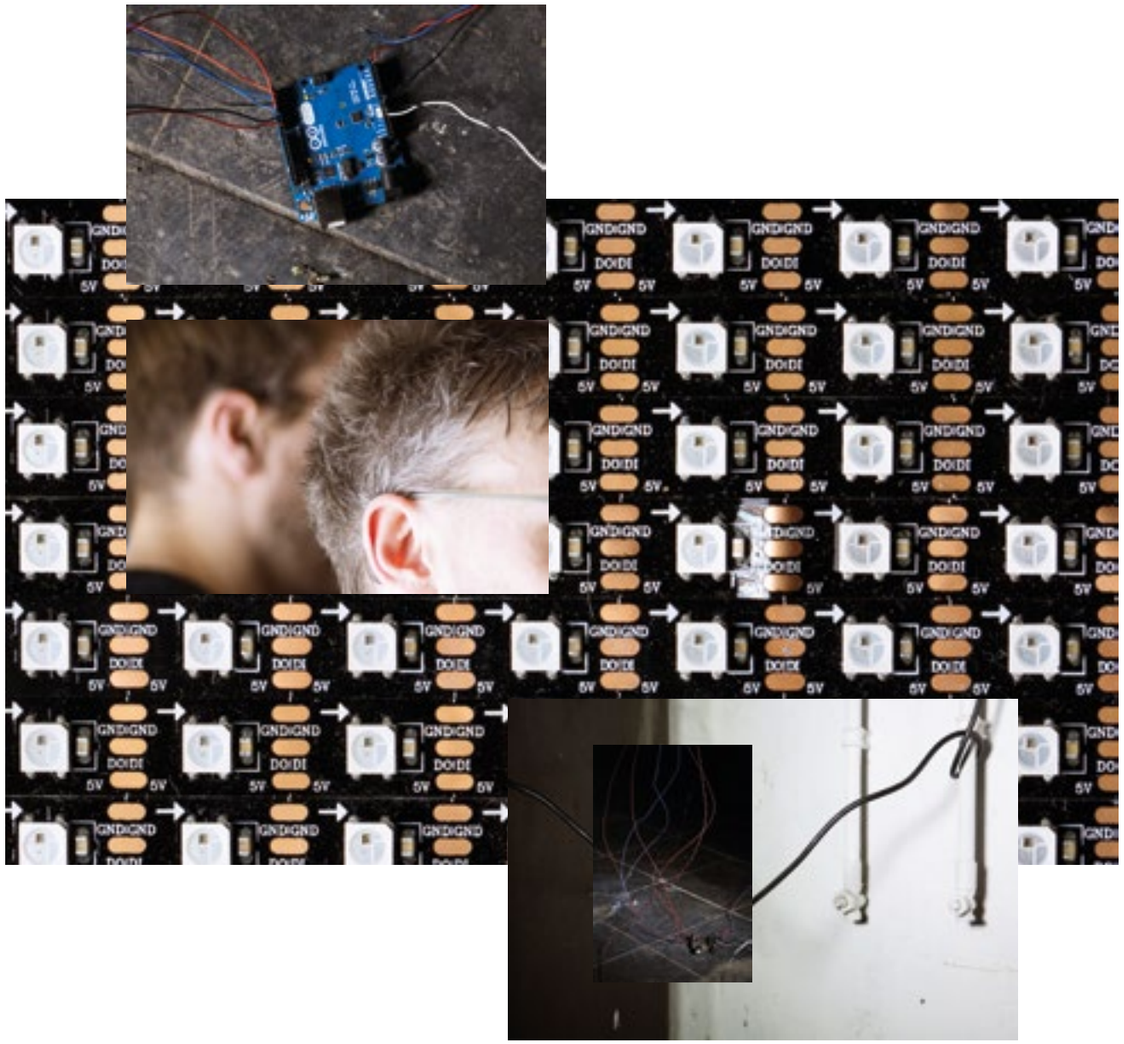
aber Informationsgestaltung für die Öffentlichkeit nicht länger unabhängig von der Gestaltung der interessierten Öffentlichkeit selbst ist, wird der Kompetenzbereich wissenschaftlicher Methodik überschritten. Soll dies nicht durch Gesten wissenschaftlicher Strenge und Selbstbeschränkung (Stichwort „Evidenzbasierung“) kaschiert oder durch Umdeutung überkommener Grenzen von Wissenschaft (Stichwort: „Mode 2-Wissenschaft“) normalisiert werden, bedarf es einer Kommunikation, die diese Überschreitung selbst noch reflektier- und handhabbar macht – und dies leistet in besonderer Weise die Kunst.

War insofern die Kontaktaufnahme zur und Zusammenarbeit mit der Kunst folgerichtig, bleibt doch noch unklar, wie diese

*Kooperation auszugestalten ist, um die kartografische Aufzeichnung der Kontroverse um Privatheit im digitalen Zeitalter der öffentlichen Reflexion zugänglich zu halten. Relativ schnell war im Team die Einsicht gereift, dass eine arbeitsteilige Zusammenarbeit, die das künstlerische Moment auf visuelle Aufbereitung wissenschaftlich bereitgestellter Analyseergebnisse reduziert, der Aufgabe nicht angemessen ist. Als Ergebnisse der Zusammenarbeit zwischen Künstler*innen, Gestalter*innen und Wissenschaftler*innen finden sich oft komplexe Diagramme von Prozessen oder Daten die den Gestaltungsgattungen Data-Visualisation oder Infographics zugeordnet werden. Hier beschränkt sich die Kooperation auf den Austausch und die Abstimmung der Arbeitsergebnisse separater Kompetenzen. Die Grauzone zwischen Kunst und Gestaltung auf der einen und Wissenschaft auf der anderen Seite wird nicht befragt und erforscht.*
Eine gemeinsame Forschung findet schon

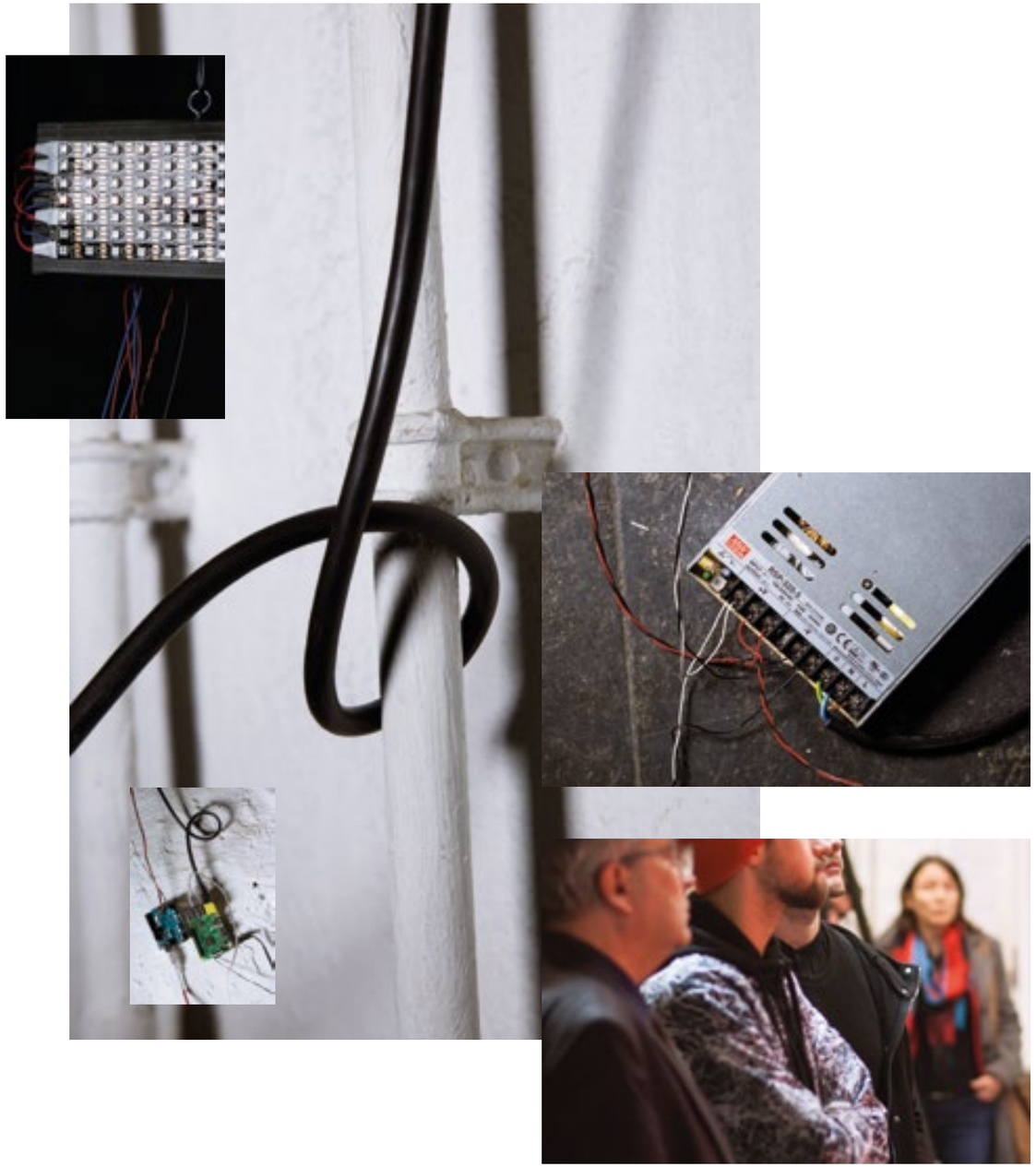
gar nicht statt. Doch legt eine auf optimierte Lesbarkeit ausgerichtete Visualisierung die Öffentlichkeit auf die Rolle eines konsumierenden Publikums fest, das sich zur eigenen Positionierung und reflektierenden Auseinandersetzung kaum herausgefordert sieht.

*Demgegenüber wurde hier der Weg einer echten Kollaboration beschritten, bei dem es nicht um bloße Illustration wissenschaftlicher Ergebnisse ging, sondern um die gemeinsame Entwicklung einer Formensprache und um eine Darstellung mit starkem Fokus auf die Erfahrbarkeit der Prozesse und Ergebnisse für das Publikum. Die Ausgangsbasis dafür ist gemeinsame Forschung, das Überschreiten von Zuständigkeitsgrenzen in gemeinsamen Untersuchungen und Experimenten, bei denen die Künstler*innen und Gestalter*innen in die umstrittene Materie der Privatheit im digitalen Zeitalter ebenso einsteigen, wie die Wissenschaftler*innen zugleich an Visualisierungs- und Gestaltungsfragen beteiligt*



werden. Die Ausstellung und das Konzept zur Darstellung basieren daher überwiegend auf gemeinsamen Erfahrungen, die von kleinen Teams aus Kunst und Wissenschaft in experimentellen Annäherungen an die Themen der Privatheit und Digitalität gemacht worden sind. Diese Experimente wurden teils direkt in die Ausstellung integriert, teils nachgestellt. Sie nehmen ihren Ausgang bei verschiedenen Lösungsvorschlägen und exemplarischen Strategien im Umgang mit digital verunsicherter Privatheit: Neben dem Vorschlag des nationalen Routings, der am Beginn des Arena-Projekts stand, waren dies die Themen Kryptografie, Europäische Datenschutzgrundverordnung, NSA-Untersuchungsausschuss sowie Big Data.

Die nachfolgenden Artikel zu diesen Themen sind entsprechend als Ergebnisse kollaborativer Bemühungen von Kunst und Wissenschaft zu lesen, eine lernende Öffentlichkeit für die Privacy-Arena zu induzieren. Sie spiegeln Zugänge wider, die auch in die Website privacy-arena.net eingeflossen sind. Um dem Publikum aber nicht nur Wissen anzubieten, sondern Erfahrungen zu ermöglichen, wurde ihm zunächst im Rahmen einer Ausstellung Raum geboten, sich nach Lust und Interesse zu betätigen und mit der Materie auseinanderzusetzen. Die Gruppe aus der Kunsthochschule hat im Vorfeld dafür Übersetzungsarbeit geleistet: Sie hat den Fragestellungen der Wissenschaft zur umstrittenen und verunsicherten Privatheit auf der technischen Ebene nachgespürt und zu verstehen versucht, wie sich Informationen mit Personenbezug durch das Netz bewegen und darin abgegriffen werden.



Diese experimentelle Auseinandersetzung hat ein tieferes technisches Verständnis für die Fragestellung der Privatheit und ihrer begründeten oder unbegründeten Überschreitung ermöglicht. Diesen Zugang sodann im Rahmen einer Ausstellung nachlebbar zu machen, diente gleichsam als Testlauf, um mit Hilfe der Begehrlichkeit exklusiver Teilnahme ein begrenztes Publikum dazu zu bewegen, den Weg zur lernenden Öffentlichkeit gemeinsam mit uns zu erproben.

Gewiss ist dieser in der vorliegenden Dokumentation festgehaltene Prozess der Kollaboration von Kunst und Wissenschaft dabei nicht viel mehr als ein erster Schritt, dem jedoch weitere folgen können.

Invisible Machines

von Mike Huntemann, Isabel Paehr, Jörn Röder

INVISIBLE MACHINES

02

In this text we question the connections between hardware, software and research outcomes brought together in an exhibition and research project titled **Privacy-Arena**. We joined the inter-disciplinary group compromising of scientists (sociology, law and ethics) from October 2015 to December 2016 to create a visual tool in the form of a web-platform in order to present and navigate through the research results.

In the process we transformed the idea and developed art instal-lations, tools and a website not only to explain and to make visible the research results of our collaborators to the public, but also to expand this research to the fields of media art and design.

1. from transparency to permeability

A key term in discussions around both computers and privacy is ‚transparency'. Transparency is the agency of different operators, for nowadays technical devices enable and disable gazes. Com-puters render users transparent to their observers and simultane-ously obscure not only the objectives of their computations but computation itself, thus becoming intransparent. According to theorist Wendy Hui Kyong Chun, modern technical devices not only obfuscate computation, but in fact hide that they (re-)generate data instead of simply represent it.

‚This notion of the computer as rendering everything transparent, however, is remarkably at odds with the actual operations of com-putation, for computers — their hardware, software, and the volt-age differences on which they rely — are anything but transparent.'[1]

1 Programmed Visions, Software and Memory, p. 17, Wendy Hui Kyong Chun

https://vimeo.com/209863927

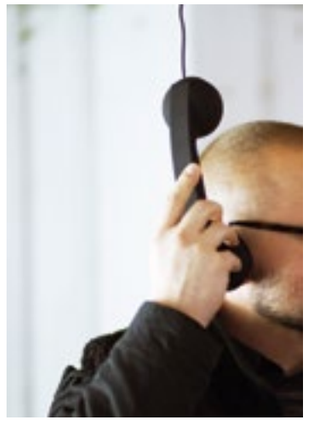
We considered this interesting because our collaborators were working with processes that had been instantiated to increase transparency such as the *NSA-Untersuchungsausschuss*. Though this inquiry committee was established to render visible the ways in which the NSA used communication data under German law; it was itself non-transparent by being inaccessible to the public. For this reason, activists called for transparency.

Although a transparent object enables light to pass through, other materials; protocols, places, bodies; remain opaque. To see through something does not necessarily mean you can use what you see. Even seeing is no longer connected to knowing.

We propose *permeability* as a more specific term and strategy than *transparency* (🤝 reaching through vs 🧿 looking through).

Permeability allows all kinds of objects to float, transform and spread through permeable barriers. When people call for transparency in the context of politics and computers, they really call for bodies and information to pass boundaries - such as for individuals to visit *NSA-Untersuchungsausschuss* meetings or to have the ability to download meeting protocols etc.

Our exhibition proposed to engage with the concept of permeability. Vistors were given free access and had the chance to become a part of the installations - in contrast to be excluded from them. For information to become accessible we imagined the visitors as participants, who would, as physical bodies, move through the exhibition space and take action. The phones hanging from the ceiling had to be picked up, and only then would they stop their irritating noise and reveal the voice of a political actor who would be talking to the visitor briefly about their individual point of view on the *European General Data Protection Regulation*. To interact with *Cryptography*, the visitors composed a message which was then sent as a light pattern through the exhibition space and regenerated in the middle of the installation as two light sequences by a laser splitter – one message encrypted via *Pretty Good Privacy (PGP)*, the other plain text. In one installation, we decided to actively break this concept of permeability: The visitors were physically separated by a glass door from a room that displayed videos dealing with big data, as a means to make the inaccessibility of what is called a ‚black box' tangible.



2. from map to network

Our collaborators' first research results we were confronted with were schematic maps with which they defined, located and brought into relation different actors. Actors were governmental or non-governmental organizations, fields of business like the media or heterogeneous groups, e.g. users. However, computers were not listed, nor were they seen as actors themselves, while they clearly structured the aesthetics of these maps: they resembled electronic circuits, all actors constructed a network, the basic idea was that invisible relations perform visible output. One could even argue that mapping itself is connected to computers as a metaphor, as every interface – especially GUIs – are considered mappings of alleged invisible processes.

The use of metaphors in design is a given. In 1923 Wertheimer defined the ‚Gestaltgesetze', which describe the perception of correlations between sizes, colours and proportions of elements within design. The size of an element can stand for the importance of what the element represents, or for the entities it comprises (e.g. how many people work in a mine) depending on the context in which it's embedded. The maps we were shown by our collaborators unwillingly ignored these correlations which made them difficult to read. Sizes and colours had been applied randomly, all elements had had to fit into a circular border (the arena), a confusing, yet to us an interesting starting point.

However, we did not see our part in improving these maps, as we were concerned that visualising the invisible using so called *information design* was a common but still compensatory gesture: To exclusively find symbols of transparency or clarity (such as pretty circles of different sizes), while the underlying processes remain obscure is to accept design as a process of finding simple images, instead of design as a practice of solving problems in the realm of the opaque, obscure and unknown. This realm was wide open: Since the research results we were asked to visualise would not be available until the very end of the funded research period, the research and our visual work were to be developed in parallel.

Another difficulty we had with the maps our collaborators had developed was that we were never quite sure wheather to categorize ourselves as artists, activists, users, coders, designers, hackers, citizens, maybe even as part of ‚the media', ‚digital industry' or ‚NGOs' and had trouble finding a spot that represented us on these maps. Over time, wouldn't our positions change? So, what if visitors could walk around between the different actors that were represented within the maps? They could actually form a network by moving through the map and connecting the different fixed points with their steps. By representing different actors with patterns and boxes on the ground, visitors could sit, read, rest and talk to each other, thereby exploring the Arena of the *European General Data Protection Regulation* our collaborators imagined - a space one could both enjoy and learn from.

For the other installations, we chose not to work with the direct idea of the Arena, but rather to use the idea of individuals in the exhibition space who would become part of the discourse around privacy by engaging with it physically and mentally. By converting the usually invisible processes of *Routing* and *Cryptography* into materials such as wood, glass, light, and by making the interaction of visitors a crucial part of the installations, we brought together the principle of routing/cryptography and the need for it in a global network.

We chose permeability as a design strategy with the aim of not finding one unifying visual truth but rather the possibility of a network in which meaning would be generated instead of reinstanciated.

3. abstraction over simplification

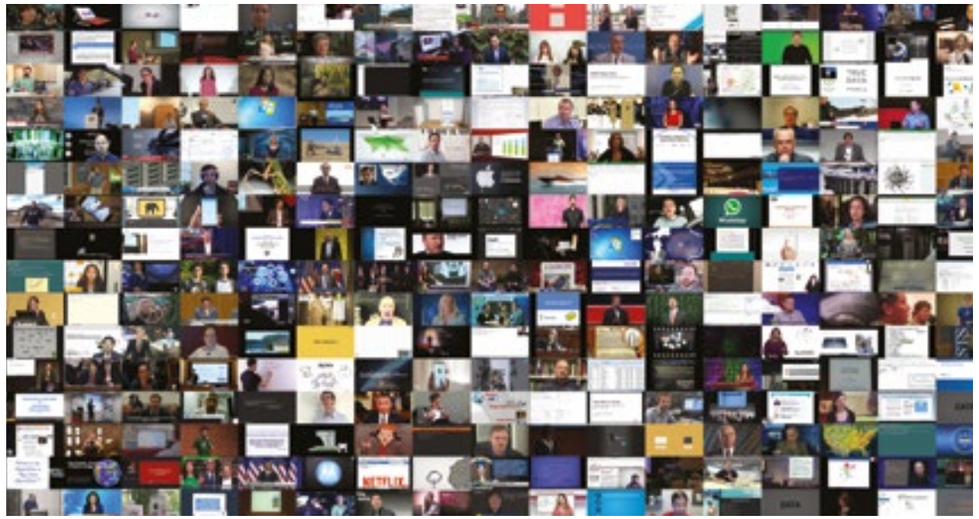
Software is structured as an interconnected graph of components where most problems are hidden in nested layers of abstraction. Breaking problems down into smaller tasks, which then have to be solved separately is a common concept. By using abstraction as a general approach, we were able to divide ourselves and our collaborators into smaller groups, ideally mixing members with different expertise and having them work together for a given time. Together we extracted starting points for further artistic questioning, finally leading to the development of installations and our website.

But how could we extract starting points for research fields like *Cryptography*, the *European General Data Protection Regulation*, the *NSA-Untersuchungsausschuss* or *big data* so visitors who may have never heard about them could communicate with? How to make visible what is called a ‚black box' or an ‚algorithm' when actually none of us can know how big data algorithms of specific companies work in detail?

When working with the invisible, one has several choices: To find artifacts that are a manifestation into matter of the intangible processes. To create imagery that works as a metaphor for the invisible. To provoke errors or irregularities by attacking the invisible through serious play and art activism.

investigating the substance of big data

To create imagery for ‚black box algorithms' we applied the same core principles and methods of big data algorithms – collection, analysis and identification to our artistic research tools. We wrote an algorithm that extracted timestamps and text snippets containing the word ‚data' from video metadata hosted on YouTube. The resulting pool of subtitle snippets was then brought in sequence by the software before the corresponding video snippets were combined into a 15 min video[2].



One could question not only the authorship of the video but the substance itself.

2 https://vimeo.com/209864062

stressing the need to use cryptography

In the exhibition space, we built a construction made of dark wood in the shape of a Y. From the single end a sequence of light patterns was shot to the center of the construction which held a prism that divided the sequence into two light rays. When these light rays hit sensors at each end of the two boards, the messages the light patterns contained were displayed on LED-boards attached to the construction. One message then got decrypted, the other remained cyphertext.

When a message like an e-mail is sent by a sender and to be received by a specified receiver, a person or organization can insert a method to copy the message for themselves to read, analyze or use in ways unknowable. That is possible with the infrastructure we built with the wood, the laser, the laser splitter / prism, a raspberry pi and arduinos as much as it is possible with transnational submarine cables, servers and personal computers. Within both infrastructures, encryption can be used not to prevent actors to access the sent data packages but to make them unreadable to everyone but the intended receiver.

Reducing material to its elemental concepts doesn't simplify the complexity of a technology or the context it is embedded in but allows to focus on the pure function, the pivotal point of the idea and its message.

4. final thoughts

In the process of working with our collaborators, we engaged with the idea of research based art and partly converted it into *art based research*. While our personal work also requires research, it has been an enriching experience for us to work with and counter to our collaborators. Being the transmitter of multiple fields and truths we often felt like an intermediary. We consider the most important part of our work that the expertise, texts and resources of the different fields involved are now available to the public.

Krypto-grafie

von Andreas Baur-Ahrens,
Thilo Hagendorff, Maria Pawelec

KRYPTO-GRAFIE

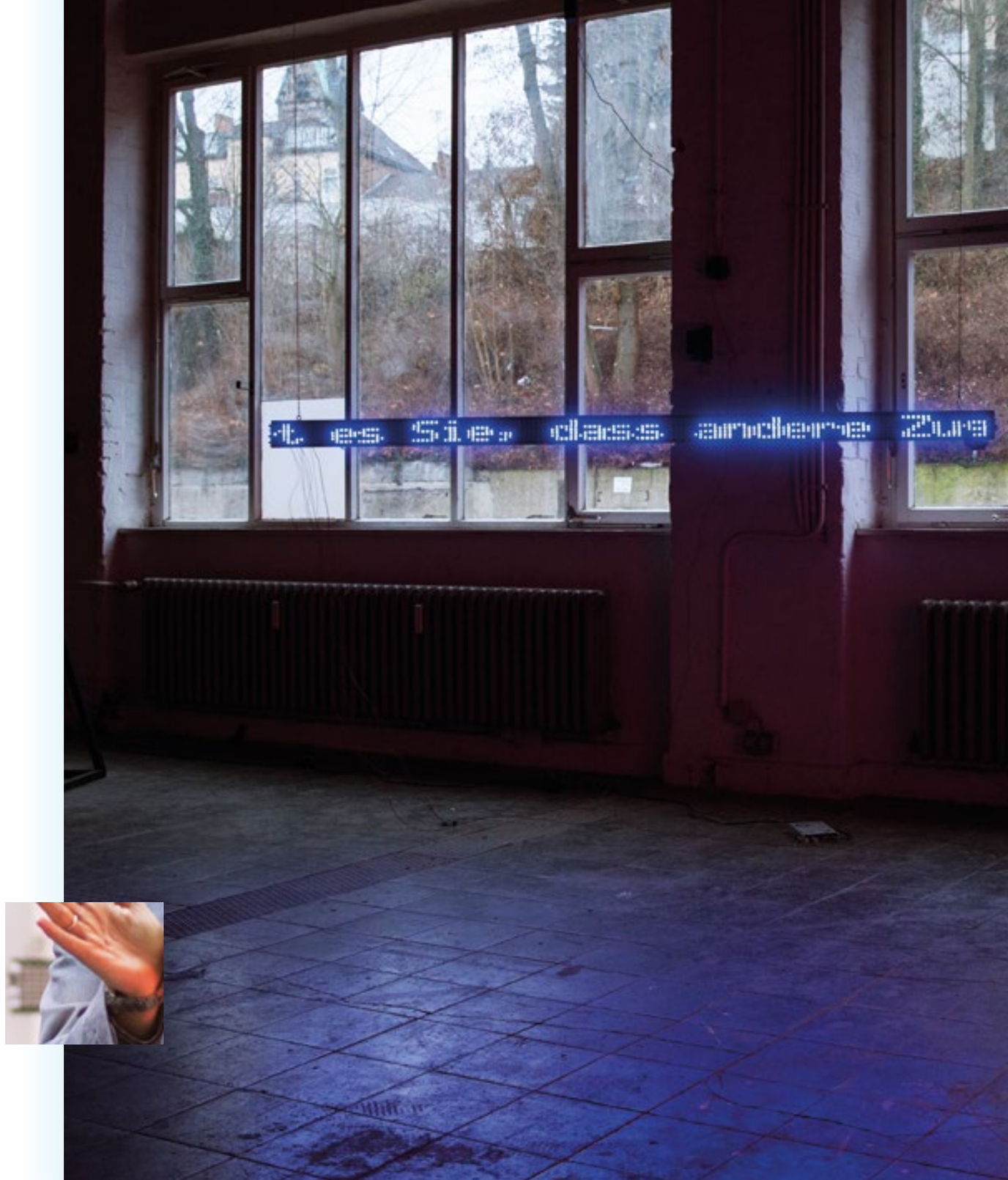
03

Kryptografie ist gerade im Anschluss an die NSA-Affäre zu einem wichtigen Thema in der Privacy-Arena geworden, um das viel gestritten wird. Zahlreiche soziale Welten wie die der IT-Wirtschaft, der Sicherheitspolitik, des Datenschutzes oder der Netzgemeinde beteiligen sich an den Aushandlungen um Kryptografie. Dabei werden verschiedene Positionen gegenüber dem genannten Streitgegenstand eingenommen. Die IT-Wirtschaft ist selbst gespalten, da Unternehmen auf der einen Seite Vertrauen durch die Kund*innen in ihre eigenen Produkte erzeugen wollen, was sich in erster Linie dann realisieren lässt, wenn angebotene Dienste und Plattformen wie etwa Messenger mit einer guten Verschlüsselung arbeiten. Auf der anderen Seite verhindert die Verschlüsselung in vielen Fällen, dass Inhaltsdaten gesammelt werden können, welche wiederum großen finanziellen Mehrwert erzeugen. Insbesondere gegenüber den Bestrebungen von Sicherheitsbehörden, welche an der Brechung oder dem Verbot von Verschlüsselungsverfahren interessiert sind, nehmen IT-Unternehmen in der öffentlichen Kommunikation in der Regel aber die Position ein, dass sie Kryptografie als wichtige Technologie verteidigen. Auch Vertreter*innen des Datenschutzes sowie der Netzgemeinde positionieren sich für Verschlüsselung, da sie als wichtiges Mittel zur Sicherung der informationellen Privatheit gesehen wird. Dabei wird jedoch mitunter außer Acht gelassen, dass kryptografische Methoden auch dazu eingesetzt werden, um handfeste Norm- und Rechtsverletzungen zu kaschieren. Insgesamt ist Verschlüsselung jedoch eine der letzten zuverlässigen Schutzmethoden gegen die immer weitreichendere „Datensammelwut" diverser wirtschaftlicher und staatlicher Institutionen. Im Rahmen der Kunstausstellung wurde die Funktionsweise von Verschlüsselung anhand einer Installation visualisiert, in der sowohl Klartext-Nachrichten als auch verschlüsselte Nachrichten nebeneinander stehen.

1. Was ist Kryptografie?
Unter den Bedingungen einer relativen Unkontrollierbarkeit von Daten- und Informationsströmen innerhalb global ausgedehnter Computernetzwerke haben sich kryptografische Verfahren als vielversprechendste Möglichkeit zum Datenschutz respektive zur Errichtung von stabilen, vor Angreifenden geschützten Informationsbarrieren bewährt.

Allgemein gesprochen basieren kryptografische Verfahren auf mathematischen Problemen, welche nur äußerst schwer beziehungsweise nur mit immensen Rechenressourcen, also ausreichend Zeit, leistungsfähigen Prozessoren, Speicher etc., rechnerisch gelöst werden können. Die Auflösung dieser mathematischen Probleme ist immer dann erforderlich, sobald man keine Berechtigung hat, auf bestimmte Informationen zuzugreifen. Andernfalls ist man – zumindest der Theorie nach – im Besitz von Schlüsseln, mit denen das mathematische Problem nicht aufgelöst werden muss. Kryptografie schafft auf diese Weise Informationssicherheit, da kryptografische Verfahren nur dann gebrochen werden können, wenn jene bislang praktisch ungelösten und nicht in Polynomialzeit auflösbaren mathematischen Verfahren doch praktisch innerhalb eines vertretbaren Zeitrahmens gelöst werden, was jedoch mit sehr hoher Wahrscheinlichkeit ausgeschlossen werden kann. Die Schwierigkeit der mathematischen Probleme garantiert die Sicherheit der Kryptosysteme.

Traditionelle kryptografische Verfahren setzen auf symmetrische Schlüsselsysteme, bei denen die Kommunikationspartner jeweils denselben Schlüssel zur Entschlüsselung übermittelter Informationen verwenden, welcher geheim gehalten werden muss. Diese Secret-Key-Kryptosysteme sind im Kontext von internetbasierten Anwendungen ungeeignet, da der Schlüsseltausch, welcher vor dem Informationsaustausch zwischen den Kommunikationspartnern durchgeführt werden muss, eine Schwachstelle darstellt, welche von Angreifern ohne größeren Aufwand ausgenutzt werden kann. Moderne Kryptografie setzt daher auf asymmetrische Public-Key-Kryptosysteme, bei denen jeweils verschiedene, also private und öffentliche Schlüssel zur Anwendung kommen.



1.1 Anwendungsarten

Es existieren verschiedene Anwendungen für Kryptografie in der informationstechnischen Kommunikation: Eine Datei- oder Festplattenverschlüsselung sorgt z.B. dafür, dass dort gespeicherte Informationen nur durch authentifizierte Personen gelesen werden können. Beispiele sind das sehr bekannte aber mittlerweile eingestellte TrueCrypt sowie BitLocker. Eine Transportverschlüsselung hingegen sorgt dafür, dass die Kommunikation zwischen einem Server und einem Client (also Computer, Smartphone o.Ä.) nicht mitgelesen werden kann und wird bei vielen Webseiten wie z.B. beim Online-Banking oder beim Zugriff auf Kundenkonten eingesetzt. Die gebräuchlichste Form der Transportverschlüsselung nennt man TLS (Transport Layer Security), in früheren Versionen auch als SSL bekannt. Die übertragenen Daten liegen aber auf dem Server bzw. beim Computer unverschlüsselt vor. Bei der Ende-zu-Ende-Verschlüsselung wird wiederum darauf Wert gelegt, dass bei einer Kommunikation zwischen zwei Geräten die dazwischenliegenden und die Daten transportierenden Server selbst ebenso wenig mitlesen können wie Fremde. PGP im E-Mail-Verkehr oder auch das Signal-Protokoll bei Smartphone-Messengern (u.a. eingesetzt bei WhatsApp) sorgen dafür, dass nur die beiden Kommunizierenden die Inhalte sehen können, nicht aber die Infrastrukturbetreiber. Natürlich sind diese verschiedenen Formen der Verschlüsselung auch kombinierbar.

1.2 Informationssicherheit

Kryptosysteme sollen die Vertraulichkeit der Kommunikation bzw. der Informationsübermittlung sichern. Deshalb spielen sie durchaus eine relevante Rolle in Debatten um Privatheit, weil häufig (aber nicht immer) Privatheit mit geschützten Informationen gleichgesetzt wird. Zudem sollen sie die Integrität der übermittelten Informationen garantieren. Vertraulichkeit bei der elektronischen Telekommunikation kann durch den Einsatz sicherer Verschlüsselungsmethoden hergestellt werden, sodass überhaupt die Bedingungen dafür geschaffen sind, dass geschützte Informationen in Datenpaketen an eine*n Kommunikationspartner*in übermittelt werden. Zudem ist die Integrität von Informationen immer dann gegeben, wenn sichergestellt werden kann, dass die Informationen bei ihrer Übermittlung über einen potentiell unsicheren Kommunikationskanal zwischen Sender*in und Empfänger*in nicht manipuliert worden sind. Darüber hinaus wird bei einigen Verfahren durch Verifizierung sichergestellt, dass die Kommunikation nur zwischen zwei untereinander ausgewiesenen Endpunkten stattfindet und sich niemand drittes als einer dieser Endpunkte ausgeben kann. Eine Interpretation der Bedeutung von Kryptografie für Privatheit schließt an Theorien der informationellen Kontexte an: Nach dieser

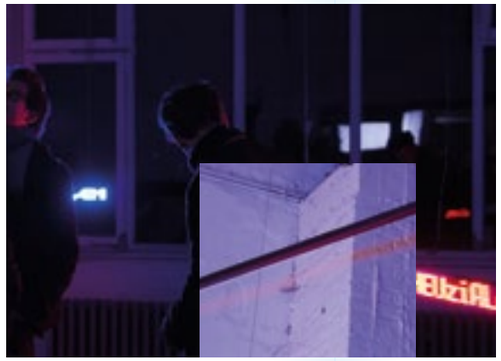
Lesart schaffen Verschlüsselungstechnologien die Bedingungen für die Herstellung von Privatheit, indem sie es ermöglichen, im Rahmen der über informationstechnische Systeme vermittelten Kommunikation unterschiedliche Informationskontexte voneinander zu trennen (Nissenbaum 2010). Durch Verschlüsselung kann z.B. der Kontext des Austauschs unter Freunden vom Kontext der Arbeit getrennt werden, oder der Kontext der Arzt-Patienten-Beziehung vom Kontext der Wirtschaft. Das bedeutet, dass kryptografische Verfahren verschiedene sozial entstandene Informationskontexte innerhalb informationstechnischer Systeme reproduzieren. Diese aufrecht erhaltenen Informationskontexte sorgen wiederum dafür, dass die jeweiligen Normen des angemessenen Informationsflusses (die bestimmen, wer Empfänger*in bestimmter Informationen sein darf und wie Informationen verbreitet werden dürfen) auch im Rahmen vernetzter informationstechnischer Systeme eingehalten werden. Kryptografische Verfahren sind daher eine der Technologien, mit welcher auf den globalen Trend der wachsenden Verbreitung von Daten- und Informationsströmen reagiert wird. Verschlüsselung spielt deshalb in Debatten um Privatheit eine große Rolle, weil sie als eine Möglichkeit verstanden wird, ein bestimmtes Verständnis von Privatheit (das der getrennten Informationskontexte) umzusetzen.

Aber auch für ein Privatheitsverständnis, das Privatheit v.a. über die erfolgreiche individuelle Informationskontrolle definiert, ist Verschlüsselung zentral. Denn sie stellt ein Instrument dar, Informationen vor anderen zu schützen und selbst zu kontrollieren, wer wann darauf Zugriff haben soll.

2. Verschlüsselung und der Staat

Der Anteil der Daten, welche sowohl im Fest- als auch im Mobilfunknetz über verschlüsselte Verbindungen ausgetauscht werden, hat in Folge der Snowden-Enthüllungen signifikant zugenommen. Das zeigen Studien, in denen erhoben wurde, welche Bandbreite verschiedene Formen des Datenverkehrs im Internet belegen. So hat sich der verschlüsselte weltweite Datenverkehr seit dem NSA-Skandal verdoppelt (Sandvine 2014).

Dennoch wird vor dem Hintergrund staatlicher Überwachungsskandale weiterhin eine Ausweitung des Einsatzes von Verschlüsselungsverfahren gefordert. Aus der Welt der Wissenschaft selbst kommt von



Kryptografen wie Rogaway die Mahnung, Kryptografie als politisches Werkzeug wiederzuentdecken und einzusetzen (Rogaway 2015). Ferner plädiert David Kaye, der Sonderbeauftragte der Vereinten Nationen für Meinungsfreiheit, für ein Menschenrecht auf Verschlüsselung. Staaten, so Kaye, sollen durch eine starke Datenschutzrechtsetzung den Einsatz von Verschlüsselung fördern, damit beispielsweise möglichen Einschränkungen des Rechts auf freie Meinungsäußerung vorgebeugt werden kann. Kaye spricht sich ferner dafür aus, dass Verschlüsselungsprogramme nicht mit Hintertüren versehen werden. Wenn staatliche Akteure überhaupt die Genehmigung dafür erhalten sollten, auf verschlüsselte Kommunikation mit der Absicht der Entschlüsselung zuzugreifen, dann dürfe dies nur im Einzelfall geschehen und nur dann, wenn es eine klare, nachvollziehbare Rechtsgrundlage dafür gebe (Kaye 2015).

Fraglich bleibt dann nur, inwieweit Staaten überhaupt technisch in die Lage versetzt werden können, nicht-kompromittierte Kryptosysteme aufzubrechen – schließlich hilft auch eine Staatsmacht nicht bei der Lösung praktisch nicht-lösbarer mathematischer Verfahren. Dennoch stellt sich grundsätzlich die Frage, ob Technologien wie Verschlüsselung nachhaltige Lösungen für soziale Probleme bieten können.

Zudem können staatliche Akteure sich zwar nicht über Verschlüsselungsroutinen hinwegsetzen, sie können jedoch über andere Wege versuchen, Zugang zu verschlüsselten Inhalten zu bekommen. So ist es in manchen Ländern wie z.B. in Großbritannien möglich, unter bestimmten Umständen Personen in Beugehaft zu nehmen und sie so zur Herausgabe des Verschlüsselungspasswortes zu zwingen.

Am Beispiel der Debatte um die Verschlüsselung im Rahmen von wünschenswerter staatlicher Strafverfolgung auf der einen und auf der anderen Seite abzulehnender staatlicher Überwachung kann man zwei große sich gegenüberstehende Positionen ausmachen, die von verschiedenen Akteuren vertreten werden. Bei der Kontroverse FBI vs. Apple lassen sich diese exemplarisch betrachten.

Der Fall FBI vs. Apple
Die Diskussionen über den Fall FBI vs. Apple brachten – neben Inhaftierungen mit dem Ziel, Verschlüsselungspasswörter zu erhalten – (wieder) weitere Möglichkeiten für Staaten auf den Tisch, Verschlüsselungssysteme zu umgehen. Das FBI wollte das iPhone des Attentäters von San Bernardino 2015 entschlüsseln, um mehr Informationen über mögliche Hintermänner und weitere Anschlagsziele zu bekommen und verklagte Apple auf Mithilfe. Zwar wollte das FBI Apple nicht dazu zwingen, die Verschlüsselung selbst zu umgehen oder das Passwort herauszugeben – beides ist nicht möglich, denn Apple kennt das Passwort des Attentäters nicht und kann auch keine mathematischen Gesetze umgehen. Stattdessen verlangte das FBI von Apple, die Schutzmechanismen bei der Passworteingabe zu schwächen. Normalerweise werden die Daten bei einem zu häufig eingegebenen falschen Passwort vom Gerät gelöscht. Schaltet man diesen Mechanismus aus, so kann das FBI unbegrenzt viele Passwörter austesten und damit letztlich an die Daten gelangen.

Apple widersetzte sich der Aufforderung des FBI und betonte öffentlich, die Sicherheit seiner Kunden nicht gefährden zu wollen. In der hochkochenden Diskussion um diesen Fall wurde daraufhin häufig gefordert, dass Unternehmen sog. Backdoors oder golden keys in Verschlüsselungen einbauen müssten. Diese Hintertüren oder Generalschlüssel sollten es zumindest staatlichen Behörden ermöglichen, verschlüsselte Daten über eigens bereitgestellte Lücken in der Verschlüsselung lesbar zu machen. Viele Gegner*innen dieser Vorschläge, sowohl aus der Wissenschaft, aber auch aus der Zivilgesellschaft, betonen, dass man eine Verschlüsselung nicht nur für bestimmte Akteure schwächen könne, sondern bei einer solchen mutwilligen Schwächung auch dem Missbrauch durch andere Angreifer*innen Tür und Tor geöffnet werden. Darüber hinaus ist es natürlich eine grundsätzliche Frage, zu welchen Daten sich staatliche Stellen Zugang verschaffen dürfen sollen. Es ist zu vermuten, dass die Debatte über „goldene Schlüssel", die staatlichen Stellen den Zugang zu verschlüsselter Kommunikation ermöglichen, und der Kampf zwischen Netzaktivist*innen, Unternehmen und bestimmten staatlichen Stellen in Zukunft weiter Fahrt aufnehmen wird.

3. Ambivalenz von Verschlüsselung
Da kryptografische Verfahren auf mathematischen Problemen basieren, die auch kapitalstarke soziale Akteure nicht ohne weiteres lösen können, sind sie relativ sicher. Dies macht sie zu dem Werkzeug der IT-Sicherheit schlechthin. Kryptosysteme dienen der Wiederherstellung von Informationskontrolle und -sicherheit. Sie schaffen Barrieren, welche Daten und Informationen nicht ohne weiteres übertreten können und sind deshalb ein häufig diskutiertes Mittel zur Erlangung und Erhaltung von Privatheit in einer digitalisierten Gesellschaft. Darüber hinaus wäre ohne Verschlüsselung ein Großteil der über das Internet abgewickelten Geschäfte wie auch der Kommunikation (auch und gerade im Unternehmensbereich) nicht möglich, da die Gefahr des Missbrauchs, der Verletzung von privaten Geschäftsgeheimnissen und Planungen zu hoch wäre. Kryptografie stärkt die Vertraulichkeit in Interaktion und Kommunikation oder ermöglicht sie erst. So ist der

Kryptografie nicht nur aus politischer Perspektive, sondern auch aus persönlicher und wirtschaftlicher Sicht ein hoher Wert beizumessen. Gleichzeitig muss eingeräumt werden, dass Kryptografie aktiv dazu benutzt wird, Straftaten zu begehen (vgl. z.B. Ransomware) oder zu vertuschen und sich vor legitimer Strafverfolgung zu schützen. Zudem bildet Kryptografie zwar einerseits mitunter die Basis für die digitale Wirtschaft, andererseits steht konsequent eingesetzte Kryptografie jedoch im Widerspruch zu vielen werbebasierten Geschäftsmodellen, da Unternehmen aus den Inhalten der Kommunikation und Interaktion von Menschen Konsumvorlieben ableiten und für ihre Werbenetzwerke verwenden. Auch für die immer bedeutender werdenden Möglichkeiten der digitalen Assistenzen (wie z.B. Siri, Alexa, Google Assistant) ist der Zugang zu den Inhalten wichtig und steht damit im Gegensatz zu Ende-zu-Ende-verschlüsselter Kommunikation.

4. Die Bedeutung von Metadaten

In der öffentlichen Debatte über die Bedeutung der Kryptografie als Schutzmechanismus gegen Überwachung und Ausspähung ist nur am Rande der Einwand zu vernehmen, dass sich sowohl Unternehmen als auch staatliche Geheimdienste zunehmend gar nicht für die Inhalte der Kommunikation interessieren, sondern auf Basis von Metadaten Rückschlüsse über die Verhaltensweisen der Personen und ihre Netzwerke ziehen. Metadaten beinhalten bei digitaler Kommunikation Informationen z.B. über die Identität der Kommunikationspartner, die Uhrzeit der Kommunikation, den Aufenthaltsort, die verwendeten Endgeräte und anderes mehr. Diese Daten können umfassende Einblicke in das Leben von Menschen geben, ohne den Inhalt der Kommunikation berücksichtigen zu müssen. So versuchte 2014 etwa ein Niederländer anhand der bei seiner eigenen Kommunikation anfallenden Metadaten zu zeigen, welche überraschenden und umfassenden Rückschlüsse sich daraus ziehen lassen (Tokmetzis 2014). Ex-NSA Chef Michael Hayden betont, dass die NSA auch auf der Basis von reinen Metadaten Menschen umbringt (ohne auf die Inhalte schauen zu müssen) und unterstreicht damit die Bedeutung dieser Daten für Überwachungs- und Profilbildungsanwendungen (Cole 2014). Einige Geheimdienstvertreter sind deswegen auch der Meinung, dass eine verschlüsselte Kommunikation ihre Arbeit kaum behindert, da sie über die dennoch anfallenden und auswertbaren Metadaten genug Informationen zur Verfügung haben (O'Neill 2016).

Gerade, weil diese Daten so sensibel sind und auch bei verschlüsselter Kommunikation anfallen, sollte die Bedeutung von Metadaten und die Möglichkeiten ihrer Verschleierung in den Diskussionen um Kryptografie berücksichtigt werden. Auch wenn z.B. die Betreiber von WhatsApp dafür gelobt werden, dass sie nun die Ende-zu-Ende-Verschlüsselung eingeführt haben, so ist dennoch zu bedenken, dass die Metadaten weiterhin anfallen und ausgewertet werden.

LITERATUR

Kaye, David (2015): Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression. Human Rights Council. http://statewatch.org/news/2015/may/un-rapporteur-freedom-opinion-expression-encryption.pdf [abgerufen am 02.06.2015].

Nissenbaum, Helen (2010): Privacy in Context. Technology, Policy, and the Integrity of Social Life. Stanford: Stanford University Press.

O'Neill, Patrick Howell (2016): Former NSA chief says U.S. can get around encryption with metadata, argues against backdoors. In: The Daily Dot. http://www.dailydot.com/politics/michael-hayden-encryption-debate-clinton-bush/ [abgerufen am 25.05.2016].

Rogaway, Phillip (2015): The Moral Character of Cryptographic Work, S. 1 – 47.

Sandvine (2014): Global Internet Phenomena Report 2H 2014. https://www.sandvine.com/downloads/general/global-internet-phenomena/2014/2h-2014-global-internet-phenomena-report.pdf [abgerufen am 30.04.2015].

Tokmetzis, Dimitri (2014): Metadaten: Wie dein unschuldiges Smartphone fast dein ganzes Leben an den Geheimdienst übermittelt. In: netzpolitik.org. https://netzpolitik.org/2014/metadaten-wie-dein-unschuldiges-smartphone-fast-dein-ganzes-leben-an-den-geheimdienst-uebermittelt/ [abgerufen am 25.05.2016].

NSA-Untersuchungsausschuss

von Fabian Pittroff

04

Amplituden der Demokratie — Der NSA-Untersuchungsausschuss des Deutschen Bundestages als demokratische Reaktion auf Verunsicherungen nach Snowden

1. Der NSA-Untersuchungsausschuss als Krisenreaktion

Die Enthüllungen des ehemaligen US-amerikanischen Nachrichtendienstmitarbeiters Edward Snowden aktualisieren in neuer Weise soziale Transformationen im Zuge der Digitalisierung. Die Veröffentlichungen bringen auf den Punkt, wie digital-vernetzte Praktiken klassische Institutionen und Routinen der Moderne erschüttern. Auch Privatheit wird in dieser Weise verunsichert. Die Krise dieses traditionellen Ordnungskonzepts hat zur Folge, dass sich Interessierte in Sorge um die Sache versammeln. Dabei herrscht kein einheitliches Verständnis vom Privaten, sondern es ist gerade die Verunsicherung der gemeinsamen Angelegenheit, die zu neuen Kontroversen um das Issue Privatheit (Latour 2007) zwingt.

In dieser Situation der Perplexität (Latour 2010: 142) lohnt es sich, von Definitionsversuchen abzusehen und stattdessen die Kontroversen zu untersuchen, in denen Privatheit als Streitsache neuverhandelt oder restabilisiert wird. Die Frage ist dann nicht nur, welche Privatheit gebraucht oder gewünscht wird, sondern auch wie Privatheit als umsorgte Angelegenheit verhandelt wird. Auf den Tisch kommt so nicht zuletzt die Frage nach den Resilienzressourcen der Politik: Welche Formen kann und wird Demokratie annehmen, um im Zuge gegenwärtiger Transformationen Privatheit neu zu formieren?[1]

Um zu erfahren, wie sich demokratische Aushandlungsformen reproduzieren oder transformieren, hat es sich bewährt, in konkrete Kontroversen einzusteigen, um fallspezifisch zu erfassen, wie die jeweils umstrittene Angelegenheit definiert und umkämpft wird. Dahinter steckt die Annahme, dass politische Aushandlungen nicht zu trennen sind vom jeweils Ausgehandelten – die umkämpfte Sache konfiguriert die Arena ihrer Aushandlung. Deshalb ist es sinnvoll, von einem Problemfall auszugehen und zu beobachten, wie dieser kollektiv erarbeitet wird: „First define how things turn the public into a problem" (Latour 2007: 5).

1.1 Der NSA-Untersuchungsausschuss als soziale Arena

Im Zentrum stehen hier die Aushandlungen im und um den NSA-Untersuchungsausschuss (NSAUA). Das Gremium von Abgeordneten wurde einberufen, um auf die Enthüllungen von Edward Snowden zu reagieren. Es soll „Ausmaß und Hintergründe der Ausspähungen durch ausländische Geheimdienste in Deutschland aufklären" (Deutscher Bundestag o. J. a). Der hier untersuchte Problemfall ist dann entsprechend das Issue der Aushandlungen dieses ersten Untersuchungsausschusses des 18. Deutschen Bundestages.[2]

Ziel meiner Analyse ist dabei eine Kartografie (Venturini 2010) dieser Kontroverse um Privatheit mit besonderer Berücksichtigung der darin mobilisierten Formen demokratischer Politik. Zu diesem Zweck nutze ich die Theorie Sozialer Welten und Arenen. Dieses „Theorie-Methoden-Bündel" (Clarke/Leigh Star: 2007) erlaubt es, die Aushandlungen des NSAUA als soziale Arena zu verstehen, in der diverse soziale Welten aufeinander treffen, um ein geteiltes Problem zu bearbeiten.

Die Theorie Sozialer Welten und Arenen geht zurück auf Anselm Strauss, der gesellschaftliche Formationen als Ansammlung sozialer Welten versteht. Soziale Welten sind Gruppen mit einer gemeinsamen Kernpraktik (Strauss 1978, 1993: 212 – 221); sie sind bestimmt durch das, was dort getan wird (Kernpraktik), wie es getan wird (Techniken) und wo es getan wird (Orte). Soziale Welten bilden typischerweise Organisationen aus und betreiben Prozesse der Authentifizierung und Legitimation (Strauss 1982). Akteur*innen in sozialen Welten sind immer auch verstrickt in Definitionsprojekte bezüglich der Frage, wie Ressourcen verteilt und Praktiken gestaltet sein sollen. Überschneidungen sozialer Welten sind zahlreich. Wenn ein Problem auftritt, das mehrere Welten betrifft, werden Konflikte oder Kompromisse wahrscheinlich. Wo soziale Welten in Aushandlungen treten, formieren sich soziale Arenen. „An arena, then, is composed of multiple worlds organized ecologically around issues of mutual concern and commitment to action" (Clarke/Leigh Star 2007: 113). Soziale Arenen sind jene virtuellen Orte, an denen sich soziale Welten rund um bestimmte Probleme versammeln, um über eine gemeinsame Welt zu verhandeln (Strauss 1993: 225 – 232).

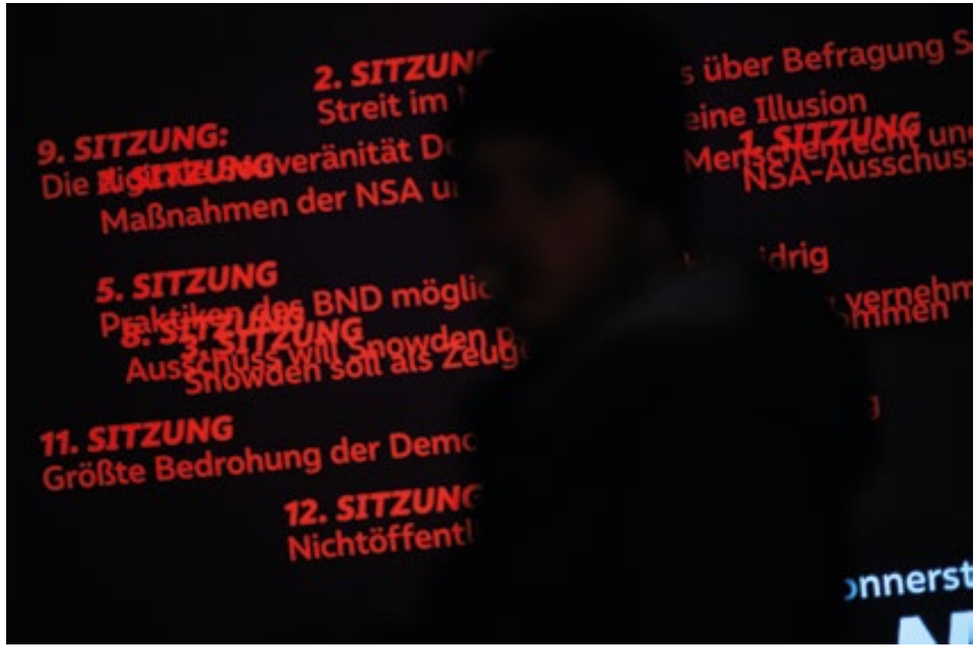
1 Mit dem Begriff „Demokratie" ist hier kein spezifisches Set an Institutionen und Routinen, sondern ein Prozess sozialen Lernens gemeint (Vgl. Marres 2007; Latour 2007; Lamla 2013).

2 Bezeichnung auf der Webseite des Bundestages: „1. Untersuchungsausschuss („NSA")" bzw. „Erster parlamentarischer Untersuchungsausschuss des 18. Bundestages" (Deutscher Bundestag o. J. a). Wird auch als „Geheimdienst-Untersuchungsausschuss" oder „NSA/BND-Untersuchungsausschuss" (Grünen-Fraktion 2016) bezeichnet.

Ich verstehe den NSAUA als Fragment der Arena aller Aushandlungen um die Krise und Neuordnung der Privatheit, d.h. als ein Segment der Privacy-Arena. Der NSAUA ist zugleich ein Segment jener Arena, die sich seit 2013 in Folge der Enthüllungen Edward Snowdens formiert hat, und ist auch in diesem Sinne Teil der Reaktionen auf die Krise der Privatheit. Doch in kaum einer Arena wird Privatheit isoliert verhandelt und auch im NSAUA geht es nie nur um Privatheit. Stattdessen sind Kontroversen um Privatheit immer eingebettet in ein Geflecht aus diversen Interessen, Werten, Techniken und Praktiken. So bekommt es die Kartografie der NSAUA-Kontroverse immer auch zu tun mit Elementen eines umfassenden Streits um die Ordnung der digitalen Welt und die Zukunft demokratischer Politik. Damit befindet sich die NSAUA-Arena an einer Schnittstelle der vielen Kontroversen um die Snowden-Enthüllungen, die Zukunft der Privatheit, die Ordnung der digitalen Welt und die Transformationspotenziale der Demokratie.

1.2 Die kollektive Suche nach Problemdefinitionen

Aufschlussreich in einer solchen Analyse ist die (teils konflikthafte, teils kompromissorientierte) kollektive Suche nach Problemdefinitionen und daran anschließenden Lösungen. Interessant sind die „struggles and negotiations to define what is problematic and what is not" (Callon 1980). So ist auch das Problem, dem sich der NSAUA widmen soll, umstritten – klar scheint nur, dass es ein Problem gibt. Damit markiert die bloße Existenz des NSAUA, dass ein Problem aufgetaucht und als solches registriert wird. Untersuchungsausschüsse des deutschen Bundestages werden fallbezogen und außerordentlich einberufen. Sie sollen es der zentralen Institution der deutschen Demokratie ermöglichen, Sachverhalte zu prüfen, „insbesondere Vorgänge, die in den Verantwortungsbereich der Regierung fallen und die auf Missstände hinweisen" (Deutscher Bundestag 2009: 1).[3] Die Einsetzung eines Untersuchungsausschusses folgt keinem Automatismus, sondern ist Ergebnis einer Problemwahrnehmung durch Teile der Abgeordneten des Bundestages. Grundsätzlich können Untersuchungsausschüsse von einer Minderheit des Bundestages (in der Regel von der Opposition) einberufen werden. Im Fall des NSAUA jedoch wurde die Einsetzung (nach längeren, größtenteils nicht öffentlichen Verhandlungen) von allen vier im deutschen Parlament vertretenen Fraktionen (Union, SPD, Grüne, Linke) beschlossen. Es bestand also Einigkeit darüber, dass ein Problem aufgetaucht ist. Aber auch zu diesem Zeitpunkt der Kontroverse ist das registrierte Problem nicht vollkommen unklar. Es hat zu tun mit den seit 2013 durch Edward Snowden und anderen öffentlich gemachten Praktiken westlicher Nachrichtendienste. Im Zuge dieser Veröffentlichungen durch den Whistleblower Snowden wurde in neuer Weise deutlich, wie umfassend Nachrichtendienste versuchen, die globale digitale Kommunikation zu speichern und auszuwerten (Rössler 2016: 104). Diese Erkenntnis generiert nicht zuletzt innerhalb der deutschen Politik neue Unsicherheit. Der Einstiegspunkt in die Kartografie der NSAUA-Arena liegt deshalb in der Analyse der kollektiven Suche nach einer Problemdefinition.



3 „Untersuchungsausschüsse […] haben die Aufgabe, politische und bürokratische Missstände in der Regierung, im Bundestag und in der Verwaltung zu prüfen und aufzuklären. […] Da der Untersuchungsgegenstand meist im Zuständigkeitsbereich der Exekutive liegt, sind Untersuchungsausschüsse vor allem ein Instrument zur punktuellen Kontrolle der Regierung" (Deutscher Bundestag o. J. b).

1.3 Zwischen Formalität und Informalität

Eine zentrale Rolle im Streit um das NSAUA-Issue nimmt der am 20.03.2014 beschlossene Einsetzungsantrag des Ausschusses ein (Deutscher Bundestag 2014a). Nicht in jeder sozialen Arena findet sich ein entsprechendes Dokument, das in ähnlicher Weise den Anspruch erhebt, das zu behandelnde Problem penibel zu umreißen. Zugleich ist der Einsetzungsantrag des NSAUA Ergebnis einer „doch sehr aufgeheizten Debatte" (Deutscher Bundestag 2014b), die durch die Verabschiedung des Antrags nicht abgeschlossen ist. Die Existenz dieses Dokuments darf deshalb nicht darüber hinwegtäuschen, dass auch nach der Einsetzung des NSAUA Uneinigkeiten über seine Aufgaben und Befugnisse fortbestehen. Interessant sind dann nicht zuletzt Differenzen zwischen dem formalen Antragsdokument und der teils informalen, praktischen Arbeit des Ausschusses.

In diesem Sinne lohnt sich ein Blick auf die formale Aufgabenbeschreibung des NSAUA: Laut Antrag soll die Frage untersucht werden, inwieweit Nachrichtendienste der Five-Eyes-Staaten (Australien, Kanada, Neuseeland, Vereinigtes Königreich, Vereinigte Staaten) Daten „von, nach und in Deutschland" erfasst haben (Deutscher Bundestag 2014a). Auf der Webseite des Bundestages heißt es: „Das Gremium […] soll Ausmaß und Hintergründe der Ausspähungen durch ausländische Geheimdienste in Deutschland aufklären" (Deutscher Bundestag o. J. a). Doch das Aufgabenspektrum ist breiter: Laut Einsetzungsantrag ist zudem von Interesse, „inwieweit Stellen des Bundes […] von derartigen Praktiken Kenntnis hatten [oder] daran beteiligt waren" (Deutscher Bundestag 2014a). Schließlich soll der Ausschuss klären, ob Empfehlungen zur Wahrung „der informationellen Selbstbestimmung [und] der Privatsphäre geboten sind" (Deutscher Bundestag 2014a). Zusammengefasst soll der NSAUA also vor allem zwei Dinge aufklären: Die Aktivitäten ausländischer Dienste und die Beteiligungen deutscher Stellen.

Mitte 2016 und damit gegen Ende der Laufzeit des NSAUA wurde der Auftrag des Gremiums auf Initiative der Oppositionsfraktionen erweitert; insbesondere um die Frage, wie der deutsche Bundesnachrichtendienst (BND) eigene Operationen (unabhängig von Kooperationen mit US-Diensten) organisiert und inwiefern die Regierung über eventuell problematische Praktiken informiert war (Deutscher Bundestag 2016a). Im Zentrum der Untersuchung stehen dabei sogenannte Selektoren, d.h. Suchbegriffe, Telekommunikationsmerkmale und Filter, mit deren Hilfe Nachrichtendienste gespeicherte Datenmengen durchsuchen (Biermann/Beuth 2015). Selektoren der NSA waren auch schon vor der Erweiterung des Untersuchungsauftrags Thema im NSAUA, Selektoren des BND darf das Gremium jedoch erst mit der Erweiterung thematisieren.[4]

1.4 Überblick über den Verlauf des Textes

Gegenstand des vorliegenden Textes ist das Issue des NSAUA; Ziel ist eine Kartografie der damit verbundenen Kontroverse um Privatheit mit besonderer Berücksichtigung der mobilisierten Demokratieformen. Dabei ist das Issue der Arena weder vollkommen klar noch unklar. Aufschlussreich ist stattdessen die kollektive Suche nach Problemdefinitionen und passenden Lösungen. Mit dem Einsetzungsantrag liegt eine erste Problemdefinition vor: Problematisch (und deshalb aufklärungsbedürftig) sind demnach die Aktivitäten ausländischer Nachrichtendienste sowie die mögliche Beteiligung deutscher Stellen an diesen Aktivitäten. Doch diese Problemfassung bleibt nicht unwidersprochen. Es sind dann die folgenden Verschiebungen des Issues, die über die Möglichkeiten und Grenzen der NSAUA-Arena Aufschluss geben.

Ich werde im folgenden Kapitel (2.) die sozialen Welten der NSAUA-Arena anhand ihrer Beziehungen, Positionen und Einsätze beschreiben. Das ermöglicht ein grundlegendes Bild der Topologie der Arena, d.h. der Möglichkeiten und Grenzen dieses politischen Raums. Dabei zeigt sich die Arena durch ein hohes Maß an Formalisierung geprägt, welches einigen wenigen Welten einen Großteil an Zugängen und Möglichkeiten gewährt. Dennoch stoßen auch die übrigen Welten Verschiebungen an, insbesondere wenn sie Kompromisse mit einflussreicheren Welten erzielen.

Im dritten Kapitel (3.) werde ich entlang einiger zentraler Ereignisse aus einer prozessorientierten Perspektive Verschiebungen des NSAUA-Issues in der Arena nachverfolgen. Während ich im zweiten Kapitel das „Gelände" der Arena erkunde, rekonstruiere ich im dritten Kapitel, welche „Bewegungen" das Issue in diesem Gelände vollzieht. Die Kartografie dieser Bewegungen zeigt, dass das NSAUA-Issue eine oszillierende Bahn beschreibt: Trotz fortschreitender Bearbeitung und inhaltlicher Transformation schwankt es

4 Mehr zur Erweiterung des Untersuchungsauftrags und der Beschäftigung mit Selektoren in Kapitel 3.4.

zwischen zwei Polen demokratischer Artikulation. Aus dieser Perspektive sind dann nicht zuletzt die Amplituden dieser Oszillation relevant: Welche Ausschläge der demokratischen Problembearbeitung sind in der Arena möglich? Wo liegen die Ränder der Arena und wie werden sie verschoben? Welche Akteur*innen werden als Teil der Arena registriert, welche als Teil des Problems?

Im vierten und letzten Kapitel (04.) werde ich schließlich zusammenfassen, welche Formen demokratischer Politik in der Arena mobilisiert werden und welche Rolle diese für die Krise der Privatheit spielen. Dabei kann ich die Oszillation des Issues und seiner Bearbeitung als Zusammenspiel zweier Modi demokratischer Politik beschreiben. Dieser Interpretation nach vollziehen sich die Problembearbeitungen in der NSAUA-Arena in einem Spannungsfeld zwischen zwei spezifischen Reaktionsformen der Demokratie, die sich zugleich stützen und blockieren. Es ist diese Konstellation demokratischer Politiken, die die Grenzen der Issue-Oszillation beschreibt und ihre Amplituden in der NSAUA-Arena definiert.

2. Topologie der Arena: Die sozialen Welten

In diesem Kapitel werde ich die wichtigsten sozialen Welten der NSAUA-Arena anhand ihre Interessen, Positionen und Beziehungen beschreiben. Eine solche Aufstellung der versammelten Welten ermöglicht einen ersten Überblick über die Topologie und die Ränder der Arena. Es soll den politischen Raum skizzieren, in dem sich mögliche Verschiebungen des Issues ereignen, die ich im nächsten Kapitel nachzeichnen werde.[5]

Die Kontroverse um das NSAUA-Issue ist nicht nur für die direkt im Ausschuss aktiven Akteur*innen relevant und die NSAUA-Arena ist nicht identisch mit dem NSAUA. Die NSAUA-Arena liegt an einer Schnittstelle diverser Aushandlungen um Privatheit, Digitalisierung und Demokratie. Um diesem Geflecht an Interessen gerecht zu werden, hilft es, die empirisch beobachtbaren Positionen und Praktiken der Akteur*innen an soziale Welten zurückzubinden. Die Perspektive der Theorie Sozialer Welten und Arenen ist hier hilfreich, insofern sie es ermöglicht, von individuellen Personen der Situation zu abstrahieren, um stattdessen die Konstellationen der Arena auf der Meso-Ebene zu erfassen.[6] So kann die soziale

5 Dieses Vorgehen bedeutet keine Verabschiedung einer Issue-zentrierten Herangehensweise. Die empirischen Analysen der sozialen Welten der NSAUA-Arena sind stets angeleitet durch die Beobachtung der kollektiven Suche einer angemessenen Problemdefinition. Welche Welten sich in der Arena versammeln, ist gekoppelt an die Form des Issues.

6 „Hier ist die Meso-Ebene die Ebene sozialen Handelns. Dies ist keine aggregierte Ebene von Individuen, sondern der Ort, wo Individuen wieder und wieder zu sozialen Wesen werden - durch Akte der Verpflichtung (commitment) gegenüber Sozialen Welten sowie ihre Teilnahme an Aktivitäten dieser Welten, indem sie Diskurse produzieren und zugleich durch Diskurse konstituiert werden" (Clarke 2012: 148).

7 Eigene ethnografische Beobachtungen um den NSAUA haben Hinweise auf einen teils vertrauten Umgang über Fraktionsgrenzen hinweg erbracht. Dieser kollegiale Umgang ist nicht das einzige Symptom einer interfraktionell geteilten Verpflichtung der Welt des Parlaments; so positioniert sich etwa auch der Ausschuss-Vorsitzende Patrick Sensburg teils gegen die Interessen der Regierung, um sich für die Rechte des Ausschusses einzusetzen, obwohl er der Unionsfraktion angehört (vgl. Kempmann/Pinkert 2015). Sensburg selbst beschreibt die Zusammenarbeit wie folgt: „Der Ausschuss hat […] eine relativ überschaubare Größe. Da lernt man sich gut kennen. Das Zwischenmenschliche passt. Sicher hat jeder seine Position, aber man schätzt einander unter Kollegen. Ich glaube, dass auch in der Sache alle Fraktionen an einem Strang ziehen" (Sensburg 2015).

8 Dafür muss nicht vollständig geklärt sein, worauf die Arbeit des Ausschusses genau abzielt. Es genügt die Verpflichtung zu einer produktiven Tätigkeit im Rahmen der grundsätzlichen Aufgabe parlamentarischer Untersuchungsausschüsse, „politische und bürokratische Missstände in der Regierung, im Bundestag und in der Verwaltung zu prüfen und aufzuklären" (Deutscher Bundestag o. J. b).

Umwelt des Ausschusses in die Analyse einbezogen werden, ohne die empirischen Spezifika der NSAUA-Arena zu sehr zu vernachlässigen. Indem Akteur*innen als Repräsentant*innen diverser sozialer Welten beschrieben werden, treten Muster kollektiven Handelns in den Vordergrund.

2.1 In der Arena zu Hause: Die Welten des Parlaments, der Opposition und der Regierung

Formal besteht der NSAUA aus acht Abgeordneten und ebenso vielen Stellvertreter*innen. Entsprechend der Kräfteverhältnisse des aktuellen Bundestages gehören von diesen 16 Personen acht zur Fraktion der CDU/CSU, vier zur SPD und jeweils zwei zu den Fraktionen „Die Grünen" und „Die Linke". Darüber hinaus sind Vertreter*innen der Bundesregierung und der Ministerien in Sitzungen anwesend, teils mit Rederecht (Biermann 2015a). In der Arbeit des Ausschusses repräsentieren diese Personen die drei zentralen Welten der Arena: Die Welt des Parlaments, die Welt der Opposition und die Welt der Regierung. In der teils stark formalisierten NSAUA-Arena verfügen diese drei Welten über zentrale Zugänge und Möglichkeiten, die andere beteiligte Welten nicht genießen – die Welten des Parlaments, der Opposition und der Regierung sind in der Arena „zu Hause".

Die Welt des Parlaments ist in der NSAUA-Arena durch die 16 Abgeordneten und Mitglieder des Ausschusses vertreten. Die Welt und ihre Praktiken sind einerseits formalisierten Abläufen verpflichtet; insbesondere Dokumente wie Sitzungsprotokolle und Anträge zeugen von streng geregelten Routinen. Aber auch informelle Praktiken sind von Bedeutung; die Akteur*innen der Welt folgen nicht nur bürokratischen Verfahrensregeln, sondern sind außerdem interessiert an produktiver Zusammenarbeit. Auch Mitglieder unterschiedlicher Fraktionen sind Kollegen*innen in der Welt des Parlaments und in diesem Sinne der gemeinsamen Arbeit im Ausschuss verpflichtet.[7] Etwa die durch alle Fraktionen beschlossene Einsetzung des Ausschusses ist Zeichen eines geteilten Interesses in der Parlamentswelt an der Bearbeitung des NSAUA-Issues (Deutscher Bundestag 2014b: 1816 – 1828).[8] Die Welt der Opposition wird repräsentiert durch die vier Vertreter*innen der Fraktionen „Die Grünen" und „Die Linke". Die Praktiken der Welt zielen darauf ab, Fehlentscheidungen von

Regierung und Regierungsfraktionen aufzudecken.[9] Untersuchungsausschüsse sind eine gute Gelegenheit, solche Verfehlungen öffentlich relevant zu machen. Mittel dafür ist mithin der Bezug auf verfassungs- und menschenrechtliche Prinzipien und Werte.[10] In der NSAUA-Arena gehört zu diesen Prinzipien auch die demokratische Kontrolle von Regierung und Nachrichtendiensten.

Die Welt der Regierung wird in der Arena durch Vertreter*innen der Bundesregierung und der Ministerien repräsentiert. Aber auch jene Ausschussmitglieder, die den Parteien der Regierungskoalition (CDU, CSU, SPD) angehören, sind der Welt der Regierung verpflichtet. Die Welt ist bemüht, einen eigenverantwortlichen Handlungsbereich (auch bezeichnet als Arkanbereich) zu bewahren, der der parlamentarischen Kontrolle entzogen ist.[11] In der NSAUA-Arena äußert sich diese Verpflichtung insbesondere als Interesse an Geheimhaltung und Opazität.[12]

Diese Dreierkonstellation sozialer Welten strukturiert die Topologie der NSAUA-Arena: Während die Interessen der Welten der Opposition und des Parlaments vereinbar und förderlich füreinander sind, verfolgt die Welt der Regierung weniger kompatible Ziele. Dabei fällt gerade jenen Ausschussmitgliedern eine Schlüsselrolle zu, die der Regierungskoalition angehören, denn sie sind sowohl der Welt der Regierung als auch der Welt des Parlaments verpflichtet. Deshalb sind sie teils blockiert durch Unvereinbarkeiten zwischen dem Interesse der Parlamentswelt an einer produktiven Arbeit des Ausschusses einerseits und dem Interesse der Regierungswelt an der Wahrung eines eigenen Handlungsbereichs mittels Geheimhaltung anderseits.[13] Entsprechend kann sich die Interessenkompatibilität zwischen Parlament und Opposition nur eingeschränkt entfalten. Auf den formalen Anspruch eines Untersuchungsausschusses hat diese Konstellation einen lähmenden Effekt, insofern die Welt der Regierung Praktiken der Prüfung und Aufklärung blockiert. So sind bestimmte Pfade für die Bewegung des NSAUA-Issues vorgegeben; gehemmt werden Transparenzansprüche, parlamentarische Kontrollkapazitäten und die reflexive Prüfung und Reformierung von Routinen.

Diese Lähmung des formalen Anspruchs des NSAUA muss jedoch nicht bedeuten, dass in der NSAUA-Arena keine produktive Arbeit am geteilten Problem geschieht. Um zu erfahren, ob und wie das NSAUA-Issue jenseits von Aufklärungsbemühungen gehandhabt wird, werde ich im dritten Kapitel entlang einiger Ereignisse der

Opposition ist ein zentraler Grund für ihre Bemühungen sicher auch die zu erwartende Aufmerksamkeit für die Arbeit des Ausschusses, sollte Snowden persönlich zu Gast sein. Snowden ist personalisiertes Symbol für eine regierungskritische Praxis, die verfassungs- und menschenrechtlichen Prinzipien verpflichtet ist (vgl. Digitalcourage 2014). Zusätzlich ist es hinsichtlich der Beziehungen zu den USA schwer vorstellbar Snowden in Deutschland Schutz zu gewähren. Somit bietet die Kontroverse eine gute Gelegenheit, die Begrenzungen der Regierung öffentlich vorzuführen. Jedenfalls hat die Opposition gemeinsam eine Klage angestrengt, um die Einladung Snowdens noch zu ermöglichen (Linksfraktion 2016).

9 In der NSAUA-Arena zeichnet sich die Welt der Opposition aus durch eine enge Zusammenarbeit der beiden Oppositionsfraktionen und durch das Ziel der öffentlichen Bloßstellung der Regierung. Paradigmatisches Beispiel für beides ist der gemeinsame Einsatz der Opposition für die Einladung Edward Snowdens als Zeugen. Eine Person aus dem Kreis der Mitarbeiter*innen der Oppositionsfraktionen nennt im Expert*innen-Interview als besonderen Misserfolg ihrer Arbeit, dass es nicht gelungen sei Snowden persönlich vor dem Ausschuss zu vernehmen.
„[…] Besonderer Misserfolg ist klar: dass man es bislang nicht geschafft hat […] den Schlüsselzeugen (gemeint ist Snowden, F.P.) […] nach Deutschland zu bekommen."
Wie wertvoll Snowden als Informant im Ausschuss auch sein mag, für die

Regierung, wir sind das Parlament, unsere Aufgabe ist es aufzuklären, unsere Aufgabe ist, die Dienste zu kontrollieren. […] Wir decken das jetzt rückhaltlos auf und ziehen dann die richtigen Konsequenzen. […] eine weitgehende interfraktionelle Zusammenarbeit […] findet nicht statt, sondern es ist dieses klassische Spiel." „Sensburg steht loyal zur Koalition. Als das Kanzleramt sich weigerte, dem Ausschuss Einsicht in jene Listen zu geben, auf denen der BND die Spionagewünsche der NSA aufgeführt hat, ließ Sensburg sich darauf ein, vorerst nur einer Vertrauensperson der Regierung Einsicht in die Listen zu geben. Doch er scheut sich nicht vor einem Streit, etwa wenn er meint, ein Zeuge dürfe zu einer bestimmten Angelegenheit aussagen, und der Vertreter des Kanzleramts anderer Meinung ist" (Lohse 2015). Christian Flisek ist einerseits für die Veröffentlichung des Datenschutzberichts über Bad Aibling (Biermann 2016a), aber andererseits gegen die Erweiterung des Untersuchungsauftrags des NSAUA (Biermann 2016b).

des NSAUA erweitert werden soll um die Frage, inwiefern der BND eigene Selektoren verwendet bzw. entfernt hat: Die Koalitionsfraktionen haben weder für noch gegen die Erweiterung gestimmt und sich stattdessen enthalten (Deutscher Bundestag 2016b: 17353). Eine Person aus dem Kreis der Mitarbeiter*innen der Oppositionsparteien sagt im Expert*inneninterview: „… bis auf den Einsetzungsbeschluss und wenige andere Initiativen wird hier kaum was interfraktionell gemacht. In Bezug auf den Untersuchungsausschuss kann man sagen, da hat man interfraktionell die Einsetzung gemeinsam beschlossen. Das war erst mal ein wichtiges Zeichen, dass das nicht die Opposition allein gemacht hat, sondern dass alle gesagt haben, wir wollen das. […] Natürlich ist es so, dass man als regierungsstellende Fraktion ein Stück weit, und das ist eben in diesem Untersuchungsausschuss sehr gut zu beobachten, immer in der Versuchung ist, die Arbeit der eigenen Bundesregierung nicht an den Pranger zu stellen. […] Aber als Unionsabgeordneter in 20 Kameras zu sagen, die Kanzlerin hat unseren Wahlkampf letztes Mal belogen, da gehört einiges an parlamentarischem Selbstbewusstsein zu. […] Wir würden uns wünschen, dass man auch auf Seiten von Union und SPD […] mit breiteren parlamentarischen Schultern an die Sache rangeht und sagt: wir sind nicht die

einen „Kernbereich exekutiver Eigenverantwortung", der verstanden wird als „ein grundsätzlich nicht ausforschbarer Initiativ-, Beratungs- und Handlungsbereich der Exekutive" (Wissenschaftliche Dienste des Deutschen Bundestages 2006: 2). Allerdings sind die Grenzen dieses Bereichs nicht klar umrissen und müssen entsprechend fallspezifisch verhandelt werden: „Die Frage, ob die Herausgabe von Informationen […] die Funktionsfähigkeit und Eigenverantwortung der Regierung beeinträchtigen, kann nicht pauschal beantwortet werden" (Wissenschaftliche Dienste des Deutschen Bundestages 2006: 4).

10 Martina Renner, Obfrau für „Die Linke" im NSAUA, sagt: „Es geht um die Zukunft unserer Grundrechte in einer digitalisierten Welt. […] Deshalb ist es für uns alleroberstes Ziel, dass der Untersuchungsausschuss so transparent und öffentlich wie möglich tagen und arbeiten wird" (Deutscher Bundestag Plenarprotokoll 2014b: 1819).
Konstantin von Notz, Obmann für „Bündnis 90/Die Grünen", sagt: „Seit knapp einem Jahr erleben wir den größten Überwachungs- und Geheimdienstskandal aller Zeiten. Die Erkenntnisse, die wir bis heute einzig und allein dem Whistleblower Edward Snowden zu verdanken haben, stehen für die Kernschmelze von Rechtsstaatlichkeit und für die Erosion der Werte Europas und der gesamten freien Welt" (Deutscher Bundestag 2014b: 1821).
Solche Prinzipien und Werte werden auch im Einsetzungsantrag des Ausschusses angeführt: So soll auch geprüft werden, ob Empfehlungen geboten sind „[…] zur Wahrung des verfassungsrechtlich gewährleisteten Schutzes der informationellen Selbstbestimmung, der Privatsphäre, des Fernmeldegeheimnisses und der Integrität und Vertraulichkeit informationstechnischer Systeme" (Deutscher Bundestag 2014a).

11 Die Bundesregierung hat einen grundgesetzlichen Anspruch auf

12 „In seiner Kompromisslosigkeit ist Wolff der sichtbare Ausdruck einer Haltung, die nicht politisch denkt, sondern bürokratisch. Das Kanzleramt wägt nicht ab, wie groß der politische Schaden einer Äußerung wäre und wie groß der gesellschaftliche Nutzen wäre, den eine Aufklärung bringen würde. Gesetz ist Gesetz und geheim bleibt geheim. Und was geheim ist, bestimmt allein die Regierung. Sie legt die Regeln fest. Wolffs Haltung kennt daher nur eine Richtung: so wenig wie möglich preisgeben" (Biermann 2015a).

13 Prägnantes Beispiel für die ambivalente Position der Koalitionsfraktionen ist das Abstimmungsverhalten zur Frage, ob der Auftrag

Situation den Transformationsverlauf des gemeinsamen Problems analysieren. Zuvor aber will ich vorbereitend einige weitere soziale Welten der Arena vorstellen.

2.2 In der Arena zu Gast: Die Welten der Nachrichtendienste, der Netzgemeinde, der Nachrichten und der Rechtsanwendung

Die Welten der Nachrichtendienste, der Netzgemeinde, der Nachrichten und der Rechtsanwendung spielen im institutionellen Setting des NSAUA jeweils sekundäre Rollen, da sie über begrenzten Zugang zu Informationen und Entscheidungen verfügen. Sie sind „zu Gast" in der Arena und nichtsdestotrotz relevant, insofern auch ihre Einsätze die Beschränkungen und Hemmungen des NSAUA-Issue ausloten und ausweiten können.

Eine Sonderstellung genießt die Welt der Nachrichtendienste. Sie wird in der NSAUA-Arena repräsentiert durch Vertreter*innen verschiedener deutscher und ausländischer Behörden.[14] Die Arbeit des NSAUA wird von den Repräsentant*innen der Nachrichtendienste mithin als Behinderung empfunden (Zeit Online 2016), aber auch als willkommener Impuls für Reformen (Biermann 2015b).[15] Die Welt ist primär Praktiken der Informationsgewinnung verpflichtet, während ihre eigene Arbeit möglichst unbeobachtet bleiben soll.[16] Vor allem innerhalb desselben Nationalstaats passt dieses Ziel zum Interesse der Regierungswelt, die eine Zone der exekutiven Eigenverantwortung pflegt. Dort sind die Praktiken der Nachrichtendienste ein paradigmatisches Beispiel für Operationen im „nicht ausforschbaren […] Handlungsbereich der Exekutive" (Wissenschaftliche Dienste des Deutschen Bundestages 2006: 2). So findet die Welt der Nachrichtendienste in der Regierung eine mächtige Alliierte und Fürsprecherin in der Arena.[17] Die Allianz dieser beiden Welten darf jedoch nicht darüber hinwegtäuschen, dass die nachrichtendienstliche Welt sich gegenüber benachbarten Welten abzuschotten versucht.[18] Während diese Abschottungsstrategie in der Regel Kompromisse behindert, fungiert sie in der Beziehung zur Welt der Regierung als Kooperationsgrundlage: Die verantwortlichen Aufsichtsinstanzen in Regierung und Bundeskanzleramt profitieren teils davon, nicht über möglicherweise rechtswidrige Praktiken des BND informiert zu werden, insofern sie bei Bekanntwerden eine Duldung oder Unterstützung solcher Praktiken plausibel leugnen können (Kurz 2016; Biermann 2017a,

15 Reformen aber weniger im Sinne einer verbesserten Kontrolle durch Regierung oder Parlament, sondern im Sinne einer materiellen oder personalen Stärkung der jeweiligen Behörde, um die operative Eigenständigkeit zu fördern (Biermann 2015b).

16 „Henry Kissinger hat einmal gesagt: Es gibt keine befreundeten Geheimdienste - es gibt nur die Geheimdienste befreundeter Nationen. Es geht nicht darum, ob jemand „gut" oder „böse" ist. Es geht um Inhalte. Und die holen wir uns" (Hayden 2016).

14 Fast alle Vertreter*innen von Geheimdiensten im Ausschuss sind Mitarbeiter*innen deutscher Dienste. Vom Ausschuss ist zwar geplant Keith Alexander und Michael Hayden, beide ehemalige Direktoren der NSA, als Zeugen zu befragen, ob die beiden US-Amerikaner aber kommen, ist noch unbekannt, denn als ausländische Staatsbürger sind sie nicht verpflichtet auszusagen. Außerdem haben William Binney, Thomas Drake und Thomas Andrew Blake bereits ausgesagt; alle drei sind zwar ehemalige Mitarbeiter der NSA, aber insbesondere als Whistleblower bekannt und entsprechend kritisch gegenüber den Praktiken der NSA. Sie können in diesem Sinne zwar als Informanten, nicht aber als Repräsentanten der Welt der Geheimdienste gelten, insofern sie ihre Verpflichtung gegenüber dieser Welt aufgegeben haben.

17 Dies gilt in erster Linie innerhalb desselben Nationalstaates, aber teils auch transnational: Die deutsche Regierung schützt in erster Linie die deutschen Dienste, aber auch die US-amerikanischen, insofern diese in wertvolle Kooperationen mit deutschen Stellen eingebunden sind.

18 Wie sehr etwa der BND an Abschottung interessiert ist, hat die Bundesdatenschutzbeauftragte Andrea Voßhoff in einem Bericht festgehalten: „Der BND hat meine Kontrolle rechtswidrig mehrfach massiv beschränkt. Eine umfassende, effiziente Kontrolle war mir daher nicht möglich" (Tagesschau.de 2016). Auch Christian Flisek, Obmann der SPD, beschwerte sich im Ausschuss über „das ‚Drei-Affen-Prinzip' des BND, nichts hören, sehen und sagen zu wollen" (Biermann 2015b).

Biermann 2017b).[19] Gleichzeitig werden innerhalb der Welt der Nachrichtendienste transnationale Kooperationen gepflegt. Die Zusammenarbeit zwischen dem deutschen BND und der US-amerikanischen NSA beispielsweise wird auch im Ausschuss nicht geleugnet, sondern von Repräsentant*innen der Nachrichtendienste und der Regierung als notwendig beschrieben.[20] Die Verflechtungen zwischen BND und NSA sind eines der zentralen Sub-Issues der NSAUA-Arena. Obwohl der Schwerpunkt des Untersuchungsauftrags laut Einsetzungsantrag auf Aktivitäten nicht-deutscher Nachrichtendienste liegt, ist auch die Frage der Beteiligung deutscher Stellen von Anfang an Teil des Ausschuss-Designs (Deutscher Bundestag 2014a). Dazu kommt, dass es für die praktische Arbeit des NSAUA einfacher ist, deutsche Beamt*innen und Politiker*innen zu einer Aussage vor dem Ausschuss zu verpflichten, als dies bei Vertreter*innen ausländischer Dienste der Fall ist.[21]

Weitere soziale Welten sind relevant, um die Politik der NSAUA-Arena zu begreifen. So ist etwa die Welt der Netzgemeinde in der Arena durch Sachverständige (Deutscher Bundestag 2014c; Chaos Computer Club 2016) und Aktivist*innen (Sueddeutsche.de 2014a) vertreten. Die Kernpraktik der Welt baut auf die Nutzung digital-vernetzter Technologien; entsprechend ist die Welt der Zugänglichkeit und Unabhängigkeit dieser Technologien verpflichtet (Ochs/Pittroff/Büttner/Lamla 2016).[22] Dies äußert sich etwa in einem Interesse an individueller Informationskontrolle und persönlichen Schutzräumen vor Überwachung (Büttner et al. 2016: 32 – 33). Neben einer grundlegenden Skepsis gegenüber staatlichen Eingriffen oder Überwachung digitaler Kommunikation setzt sich die Netzgemeinde in der NSAUA-Arena vor allem für mehr Transparenz der Ausschussabläufe ein, etwa durch Protokollierung öffentlicher Sitzungen (Netzpolitik.org; Biermann 2014a), journalistische Formate der Berichterstattung (Technischen Aufklärung 2015) oder die unautorisierte Veröffentlichung ausschussinterner Dokumente (Wikileaks 2015b). Es sind insbesondere diese Praktiken der Netzgemeinde, die die Transparenzgrenzen der NSAUA-Arena herausfordern und erweitern. Sie markieren nicht nur formale Grenzen der Issue-Bearbeitung, sondern erweitern auch den Spielraum, in dem das Issue in der Arena erfasst wird.

Die Welt der Nachrichten ist durch eine Reihe von Journalist*innen vertreten, die über den Ausschuss berichten und Sitzungen von der Besucher*innentribüne aus beobachten (z.B. Zeit Online o. J.; Süddeutsche.de o. J.; Golem o. J.). Wie die Netzgemeinde ist auch die Welt der Nachrichten an der Berichterstattung über die Abläufe in der Arena interessiert, setzt dabei aber auf journalistischere Formate, d.h. auf eine stärkere Auswahl und Vermittlung. Neben diesem allgemeinen Interesse zeigt die Welt außerdem arena-spezifischen Einsatz zum Schutz der eigenen Kernpraktik: Mithin in Reaktion auf die Arbeit des NSAUA wird von der Bundesregierung eine Reform des BND vorgeschlagen (Bundesregierung 2016). Berufsverbände der Welt der Nachrichten positionieren sich öffentlich gegen diesen Gesetzesentwurf und dadurch gegen staatliche Überwachung von Journalist*innen weltweit (Deutscher Journalisten-Verbund 2016; Reporter ohne Grenzen 2016a). Dabei geht es ausdrücklich darum, nicht-deutsche Journalist*innen vor einer Überwachung durch den BND zu schützen. So steht die Welt der Nachrichten in der Arena für ein Interesse an mehr Transparenz bei der Bearbeitung des Issues. Dabei bezieht die Welt eine explizit grund- und menschenrechtliche Position. Beide Ziele passen zu den Zielen der Opposition und der Netzgemeinde.

Auch die Welt der Rechtsanwendung positioniert sich in der Arena teils grund- und menschenrechtsorientiert. Prominent repräsentiert ist die Welt durch verfassungsrechtliche Experten, die am 22.05.2014 als Sachverständige im Ausschuss gehört werden (Deutscher Bundestag 2014d). Die Sachverständigen vertreten im Ausschuss einhellig die Position, der BND operiere teils grundgesetzwidrig. So widersprechen die Experten der Rechtsauslegung des Nachrichtendienstes, nach der der Schutz durch Artikel 10 des Grundgesetzes nur deutschen Bürger*innen zukomme.[23] Aber auch Jurist*innen des BND sind im Ausschuss vertreten, die etwa die Rechtsauslegung der Behörde darlegen (Deutscher Bundestag 2014e; Sueddeutsche.de 2014b).

3. Oszillation des Issues: Ereignisse und Verschiebungen

Das vorangegangene Kapitel hat einen grundlegenden Überblick über die Topologie und Ränder der Arena eröffnet. Im Folgenden werde ich entlang einiger Ereignisse aus einer verlaufsorientierten Perspektive die Bewegungen des NSAUA-Issue in dieser Arena nachzeichnen. Dabei beschreibt das Issue eine oszillierende Bahn: Mit fortschreitender Bearbeitung und Transformation schwankt

19 Bundeskanzlerin Angela Merkel sagt im NSAUA: „Ich wurde davon nicht informiert. Das, was sie von mir hören können, ist, was ich wusste. Und ich wusste davon nichts" (Biermann 2017b). Distanz zwischen Regierung und Nachrichtendiensten wird etwa durch das „Need-to-know-Prinzip" aufrechterhalten. Ein Mitarbeiter des BND beschreibt das Prinzip im Ausschuss: „Das ist zumindest ein sehr lange und sehr intensiv im BND […] geprägter Begriff, wo es eine Art Abschottung gab und letztendlich sehr intensiv nur diejenigen Leute an Informationen beteiligt wurden, die tatsächlich mit dem Vorgang etwas zu tun hatten" (Wikileaks 2015a: 48; Netzpolitik.org 2015).

20 Der ehemalige BND-Präsident Gerhard Schindler „betont mehrfach, wie wichtig der BND sei und wie unverzichtbar die Hilfe der NSA – für den BND und für Deutschlands Sicherheit. ‚Wir brauchen die Zusammenarbeit mit der NSA'" (Biermann 2015b). Heinz Fromm, ehemaliger Präsident des Bundesamts für Verfassungsschutz (BfV) sagt im Ausschuss, es gäbe gemeinsame Sicherheitsinteressen zwischen BND und NSA (Biermann 2016d). Hans-Georg Maaßen, aktueller Präsident des BfV, „erklärte […], warum seine Behörde die Software XKeyscore des US-Geheimdienstes NSA zur Analyse von Daten in Deutschland nutzt: Die eigenen Möglichkeiten zur Datenanalyse reichten nicht" (Zeit Online 2016). Biermann (2016c) über die Aussage von Frank-Walter Steinmeier vor dem Untersuchungsausschuss: „Sein immer wieder vorgetragenes Hauptargument: Die Kooperation mit den USA sei alternativlos, um Deutschland vor Terroristen zu schützen."

21 Insgesamt hat dies eine Verschiebung der Ausrichtung der NSAUA-Arena und eine Transformation des NSAUA-Issues ermöglicht: Während anfangs vor allem ausländische Dienste im Mittelpunkt der Ausschussarbeit standen, haben die Aktivitäten deutscher Stellen zunehmend an Bedeutung gewonnen. So hat sich der Vektor des NSAUA-Issues verschoben: Trotz der lähmenden und verschleiernden Kraft der Regierungswelt ist (über die Erkenntnis der Verflechtung) die Beteiligung deutscher Routinen an der Problemsituation gestiegen. Dazu mehr im dritten Kapitel.

22 Chaos Computer Club (o. J.); Lobo 2012; Seemann 2011; Seemann 2013.

23 Hans-Jürgen Papier, verfassungsrechtlicher Sachverständiger im NSAUA, sagt: „Artikel 10 schützt als Menschenrecht und damit gemäß seinem weiten personellen Schutzbereich nicht nur Deutsche, sondern auch Ausländer" (Deutscher Bundestag 2014f: 16). Artikel 10 greift oder nicht, haben meine Vorredner das Nötige gesagt: Er greift - richtigerweise. Es gibt keinen überzeugenden Grund für die Annahme, dass eine Telekommunikationsüberwachung im Ausland nicht unter Artikel 10 fallen soll - was dazu führt, dass diese Auslandsüberwachung durch den Bundesnachrichtendienst nach gegenwärtigem Recht unzulässig ist und die entgegenstehende behördliche Praxis rechtswidrig ist" (Deutscher Bundestag 2014f: 6). Wolfgang Hoffmann-Riem, verfassungsrechtlicher Sachverständiger im NSAUA, sagt: „Dabei sind - insofern stimme ich Herrn Papier voll zu - die hier betroffenen deutschen Kommunikationsgrundrechte nicht auf den Schutz Deutscher begrenzt, und der Schutzbereich ist territorial nicht auf Deutschland begrenzt" (Deutscher Bundestag 2014f: 10). Matthias Bäcker, verfassungsrechtlicher Sachverständiger im NSAUA, sagt: „Zu der Frage, ob

der Modus der Problembearbeitung immer wieder zwischen zwei Polen demokratischer Politik. Interessant sind dabei nicht zuletzt die Amplituden dieser Bewegung, d.h. die spezifischen Beschränkungen und Möglichkeiten im demokratischen Umgang mit dem Problem. Hier liefern gerade auch die Einsätze und Anliegen weniger einflussreicher Welten der Arena Anhaltspunkte für die Spielräume der Issue-Bearbeitung.

3.1 Die Irritation der Snowden-Enthüllungen

Am Anfang stehen die Enthüllungen von Edward Snowden. Sie sorgen auch in der deutschen Politik für Irritationen, insofern öffentlich wurde, wie umfassend Nachrichtendienste versuchen Daten zu sammeln und auszuwerten. Neu ist insbesondere die Kenntnis über Ausmaß und Anspruch, mit dem Geheimdienste das Internet überwachen wollen. Entsprechend registrieren auch Abgeordnete des Deutschen Bundestages eine (noch diffuse) Krisensituation. In Reaktion wird von diversen Seiten die Aufklärung ausländischer Datensammelpraktiken gefordert (Deutscher Bundestag 2013a). Insbesondere Repräsentant*innen der Opposition und der Netzgemeinde wollen außerdem die Rolle deutscher Nachrichtendienste und Regierungen in die Untersuchung einbeziehen.[24]

Die Einsetzung eines Untersuchungsausschusses zur Bearbeitung des neuen Problems wird anfangs nur von Seiten der Opposition forciert, während Vertreter*innen der Regierung und der Koalitionsfraktionen der Option Untersuchungsausschuss skeptisch bis kritisch gegenüberstehen.[25] Als Alternative zu einem Untersuchungsausschuss wird eine Prüfung durch das Parlamentarische Kontrollgremium (PKGr) lanciert, also eine stärker in Routinen verhaftete Bearbeitung im Rahmen einer ohnehin bestehenden Institution des Parlaments. Es sind vor allem Repräsentant*innen der Welt der Regierung, die sich für letztere Herangehensweise einsetzen.

In dieser ersten Phase der Irritation dreht sich der Streit im Bundestag um die Frage, ob zur Problemerfassung eher etablierte (PKGr) oder eher reflexive Routinen (Untersuchungsausschuss) aktiviert werden sollen. Außerdem finden sich schon zu diesem Zeitpunkt zwei konkurrierende Ausrichtungen der Problembeschreibung, die auch im weiteren Verlauf der Kontroverse von Bedeutung sein werden. So besteht Uneinigkeit darüber, ob das Problem weitgehend durch ausländische Akteur*innen verursacht wird oder ob auch deutsche Institutionen beteiligt sind, und entsprechend in die Untersuchung einbezogen werden sollten. Hier manifestiert sich ein Konflikt um die Ränder der Arena: Die Frage ist, was in die kommende Problembearbeitung einbezogen werden soll und was nicht.

3.2 Zuschnitt des Problems auf dem Weg zur Einsetzung

Bis Februar 2014 einigen sich alle Fraktionen des Bundestages darauf, dass ein Untersuchungsausschuss eingesetzt werden soll (Deutscher Bundestag 2014g: 1066 – 1077). Die Option Untersuchungsausschuss hat sich durchgesetzt und die Bearbeitung des Issues hat eine erste Formvorgabe erhalten. Die zentrale Institution der deutschen Demokratie initiiert eine relativ außerordentliche Reaktion – routiniert zwar, insofern die Einsetzung von Untersuchungsausschüssen gesetzlich formalisiert ist (PUAG 2001), aber auch außerordentlich, insofern Untersuchungsausschüsse explizit als Krisenreaktionen konzipiert sind: Durch öffentliche Beweiserhebungen sollen Probleme aufgedeckt und ggf. Reformen angestoßen werden (Deutscher Bundestag). Diese Entscheidung für einen Untersuchungsausschuss kann als vorläufiger Kompromiss zwischen den Welten des Parlaments und der Opposition (und zuungunsten der Regierung) gelten: Das Parlament kann außerordentliche Aufmerksamkeit für die Bearbeitung des entdeckten Problems vorweisen, während die Opposition die Chance hat, Verfehlungen aufzudecken, die die Welt der Regierung schwächen könnten. Die Welt der Regierung dagegen muss Angriffe und Einblicke in den Arkanbereich befürchten (Wissenschaftliche Dienste des Deutschen Bundestages 2006: 2).

Die Kontroverse über eine angemessene Problemdefinition ist mit diesem ersten Kompromiss jedoch nicht aus der Arena verschwunden, sondern verlagert sich auf Fragen nach den Gegenständen und Zuständigkeiten des Ausschusses. So legen die Koalitions- und die Oppositionsfraktionen zwei konkurrierende Einsetzungsanträge vor (Deutscher Bundestag 2014h; Deutscher Bundestag 2014f). Damit signalisiert zwar die Welt des Parlaments ihren Willen zu einem Ausschuss, schließt sich aber auch nicht vollständig der Problemdefinition der Opposition an und lässt Raum für Kompromisse mit der Welt der Regierung. So zeigt die Vorlage eines konkurrierenden

Aufklärung der Affäre auszustatten" (Deutscher Bundestag 2013c).

24 Oppositionsabgeordneter Hans-Christian Ströbele über die Aufgabe des kommenden Untersuchungsausschusses: „Aber dieser Ausschuss hätte in erster Linie die Aufgabe herauszufinden, was die deutschen Dienste gemacht haben, vielleicht mit der NSA zusammen. Zweitens sollte er klären, was die deutschen Dienste und die Bundesregierung gewusst haben" (Deutscher Bundestag 2013b).

25 „Skeptisch äußerte sich der [sic] Steinmeier [zu dieser Zeit SPD-Fraktionsvorsitzende] gegenüber der Forderung nach einem Untersuchungsausschuss des Bundestages. Es bestehe die Gefahr einer großen Selbsttäuschung, da die Verantwortlichen in den USA wohl nicht bereit seien, vor einem deutschen Untersuchungsausschuss auszusagen. Es sei besser, das PKGr mit mehr Mitteln und Möglichkeiten zur

Bundestag 2014h), nennt die Koalitionsfraktionen ihren Antrag „Einsetzung eines Untersuchungsausschusses NSA" (Deutscher Bundestag 2014i). Hier wiederholt sich die Uneinigkeit darüber, inwieweit deutsche Institutionen am Problem beteiligt sind und inwieweit sie in die Untersuchung einbezogen werden sollten.

26 Die notwendige Vermittlung zwischen den beiden Dokumenten kostet dem Parlament Zeit, die für die Arbeit des Ausschusses genutzt werden könnte. Außerdem gibt es inhaltliche Unterschiede. Die erste Differenz zwischen den beiden Anträgen findet sich schon in ihrer Bezeichnung. Während der Antrag der Oppositionsfraktionen „Einsetzung eines Untersuchungsausschusses" heißt (Deutscher

Antrags auch, dass ein Großteil der Parlamentarier*innen als Mitglieder der Koalitionsfraktionen auch der Welt der Regierung verpflichtet sind.[26]

Gut einen Monat nach Vorlage der zwei konkurrierenden Anträge verabschiedet der Bundestag ein gemeinsames Dokument (Deutscher Bundestag 2014a; Deutscher Bundestag 2014b: 1816 – 1828). Dieser Einsetzungsantrag ist ein weiterer vorläufiger Kompromiss um den Zuschnitt des NSAUA-Issue. Das neue Gremium bekommt den Namen „1. Untersuchungsausschuss (‚NSA')" (Deutscher Bundestag o. J. a) und soll dem Kompromissantrag nach die Aktivitäten nicht-deutscher Dienste sowie die mögliche Mitwirkung deutscher Stellen an solchen Operationen prüfen. Der Ausschuss ist damit formal auf die Untersuchung einer externen Bedrohung (nicht-deutsche Nachrichtendienste) ausgerichtet, gegen die ggf. Schutzmaßnahmen entwickelt werden sollen.[27] Institutionen des deutschen Staates kommen nur indirekt in Frage, nämlich wenn sie an Operationen ausländischer Dienste beteiligt sind.

Das Issue hat hier einen weiteren Zuschnitt erfahren: Das Problem, dem sich der NSAUA widmen soll, wird tendenziell außerhalb der deutschen demokratischen Institutionen verortet. Nur indirekt sollen die politischen und behördlichen Routinen des deutschen Staates eine Rolle spielen. Dem formalen Anspruch an einen Untersuchungsausschuss (Aufklärung nach innen) wird diese Anlage nur teilweise gerecht. Andererseits bestimmt die im Einsetzungsantrag dokumentierte Problemdefinition nur formal die Ausrichtung des Ausschusses. Das Dokument bedeutet nicht, es gäbe keine Dissident*innen mehr in der Arena, die diese Definition im weiteren Verlauf angreifen oder modifizieren.

3.3 Verschiebungen im Laufe der Arbeit

Ein halbes Jahr nach Beginn der Arbeit des NSAUA (04.10.14) veröffentlichen die Süddeutsche Zeitung, NDR und WDR einen Bericht über die „Operation Eikonal" (Mascolo/Leyendecker/Goetz 2014). Demnach soll der BND Daten am Frankfurter Internetknoten DE-CIX abgegriffen und an die NSA weitergegeben haben. Zumindest wenn darunter Daten deutscher Bürger*innen waren, wäre die Kooperation eine Grundrechtsverletzung durch deutsche

27 Diese Ausrichtung des Ausschusses auf den Schutz vor einer äußeren Bedrohung (im Gegensatz zur Aktivierung reflexiver Reformen im Inneren) zeigt sich auch in Abschnitt B. III. des Kompromissantrags. Dort heißt es, der Ausschuss soll klären, „ob Empfehlungen zur Wahrung des verfassungsrechtlich gewährleisteten Schutzes der informationellen Selbstbestimmung, der Privatsphäre, des Fernmeldegeheimnisses und der Integrität und Vertraulichkeit informationstechnischer Systeme sowie der sicheren und vertraulichen Kommunikation in der staatlichen Sphäre geboten sind" (Deutscher Bundestag 2014a).

Behörden.[28] Der Pressebericht ist nicht der erste Hinweis auf eine möglicherweise problematische Zusammenarbeit von BND und NSA (Fennen 2013; Geist/Gjerding/Moltke/Poitras 2014). Dennoch markiert die Veröffentlichung eine Verschiebung des NSAUA-Issue. Obwohl die Routinen des deutschen Staates bei der Einrichtung des NSAUA nicht im Zentrum stehen, kommen im Zuge der Eikonal-Veröffentlichungen zunehmend auch der BND und seine politische Aufsicht (Welt der Regierung) als Teil des NSAUA-Problems in Frage (Meister 2017). Deshalb spielen auch die Verfahren und Technologien deutscher Stellen eine immer größere Rolle in der NSAUA-Arena.[29] Presseberichte entnehmen aus Dokumenten des BND, die Identifikation und Ausfilterung von Daten, die Deutsche betreffen, hätte nie fehlerfrei funktioniert (Mascolo 2014; Biermann 2014b). BND-Vertreter*innen dagegen widersprechen in öffentlichen Sitzungen des Ausschusses diesen medialen Darstellungen (Deutscher Bundestag 2014j).[30] Ein halbes Jahr nach den Eikonal-Veröffentlichungen und ein Jahr nach Arbeitsbeginn des Ausschusses (23.04.15) erhärtet und erweitert sich der Verdacht, der BND hätte wissentlich und grundrechtswidrig Daten an die NSA weitergegeben (Baumgärtner/Gude/Rosenbach/Schindler 2015; Biermann/Beuth/Steffen 2015).[31]

Die Eikonal-Veröffentlichung markiert außerdem die Rolle der Welt der Nachrichten in der Arena. Einerseits fördern die Berichte über Eikonal eine Verschiebung des Issues, in dem sie deutlich machen welche Akteur*innen bisher unbeachtet aber relevant für das Problem sind. Andererseits gibt es Hinweise darauf, dass die Eikonal-Berichte selbst erst durch die Arbeit des Ausschusses ermöglich wurden. Ein Vertreter der Regierung legt nahe, die Berichte zu Eikonal beruhten auf streng geheimen Dokumenten, die dem Ausschuss zur Verfügung gestanden hätten und über diesen an die Presse gelangt seien.[32] Einige Tage später droht das Kanzleramt den Mitgliedern des NSAUA mit einer Klage, falls noch einmal vertrauliche Dokumente der Regierung über den Ausschuss an die Öffentlichkeit dringen sollten (Zeit Online 2014). Es scheint also Verflechtungen und gezielten Informationsaustausch zwischen der Welt der Nachrichten und den Welten des Parlaments bzw. der Opposition zu geben. Ähnliches gilt vermutlich für die Welt der Netzgemeinde, denn auch diese gelangte mehrfach an interne Dokumente des NSAUA (Meister 2014a; Wikileaks.org 2015b; Meister 2016a).

Denmark, and the Danish citizens as they transit Germany, all the while considering it entirely in accordance with their agreements. Ultimately, each EU national government's spy services are independently hawking domestic accesses to the NSA, GCHQ, FRA, and the like without having any awareness of how their individual contribution is enabling the greater patchwork of mass surveillance against ordinary citizens as a whole" (Snowden 2014).

29 Unter den technischen Systemen wird etwa das Filtersystem „Dafis" im Zuge der Eikonal-Berichte relevant für die Problembearbeitung: Mit dieser Technik hat der BND (wohl vergeblich) versucht, Daten deutscher Bürger*innen auszusortieren, damit solche Daten nicht an die NSA weitergegeben werden. „Das Vorhaben [Eikonal]

member state like Denmark may give the NSA access to a tapping center on the (unenforceable) condition that NSA doesn't search it for Danes, and Germany may give the NSA access to another on the condition that it doesn't search for Germans. Yet the two tapping sites may be two points on the same cable, so the NSA simply captures the communications of the German citizens as they transit

28 Die Praktik der bilateralen Datenweitergabe könnte auch bei perfekter Ausfilterung der Daten der jeweils eigenen Staatsbürger*innen relevant für das Problem sein, insofern dieses Vorgehen nationale Konzepte und Lösungsvorschläge gegen ausländische Nachrichtendienste unterläuft. So schreibt Edward Snowden gegenüber dem Europäischen Parlament: „The result is a European bazaar, where an EU

der Bundesregierung zur Verfügung gestellt worden sind, in kürzester Zeit in die Presse gekommen sind und sie offensichtlich Hintergrund der Berichterstattung in der Süddeutschen Zeitung waren" (Deutscher Bundestag 2014k: 5180).

geflossen" (Wikileaks 2015c: 9, 16; Meister 2014b).

31 „Das deutsche Kanzleramt hat es entweder gewusst und gebilligt, dann hätte die Bundesregierung, allen voran der damalige Kanzleramtsminister Frank-Walter Steinmeier, Gesetze gebrochen und Grundrechte verletzt. Oder der BND sagte es dem Kanzleramt nicht, dann wäre er unkontrollierbar und darf so in einem Rechtsstaat nicht existieren. […] ‚Eikonal' ist der Albtraum der Demokratie" (Biermann 2015c).

32 Klaus-Dieter Fritsche, Staatssekretär im Kanzleramt, sagt im Plenum des Bundetages: „Zunächst einmal, Frau Abgeordnete, bedauere ich es ausdrücklich, dass Unterlagen, die bis zu Streng Geheim eingestuft waren und dem Untersuchungsausschuss vonseiten

scheiterte daran, dass es technisch nicht möglich ist, eine absolute und fehlerfreie Trennung von geschützter und ungeschützter Kommunikation zu erreichen" (Mascolo/Leyendecker/Goetz 2014). Die Funktionsweise des Filters war entsprechend auch Thema im Ausschuss (Deutscher Bundestag 2015a: 10 – 13).

30 Zwei Wochen nach den Eikonal-Veröffentlichungen widerspricht ein BND-Mitarbeiter unaufgefordert dem Presseberich in einer Ausschusssitzung: „Im Regelfall kommentiere ich nichts, was in der Presse steht. Nur, diese Aussagen, wir hätten massenhaft Daten von Deutschen gesetzwidrig weitergegeben, möchte ich auf jeden Fall korrigieren. In der Zeit, in der ich verantwortlich war da draußen, ist kein Datum eines Deutschen an einen anderen Nachrichtendienst

3.4 Transformation mit Kompromissen

Mitte 2015 und im Zuge neuer Erkenntnisse über die Verfehlungen im Rahmen der Operation Eikonal erhärten sich nicht nur frühere Vermutungen. Außerdem treten neue, nicht-menschliche Akteur*innen in die Arena (Callon 2006; Lamla 2013: 98 – 107): Relevant für die Aushandlungen werden sogenannte Selektoren, also Suchbegriffe wie Telefonnummern, Email- oder IP-Adressen (Baumgärtner/Gude/Rosenbach/Schindler 2015; Biermann/Beuth 2015). Der BND durchsucht und sortiert die am Internetknoten DE-CIX gesammelten Daten mittels Selektoren. Dabei werden einerseits Selektoren verwendet, die von der NSA bereitgestellt werden, andererseits solche, die der BND für ihre eigene Erfassung einsetzt. Diese Praxis wurde als problematisch und rechtswidrig wahrgenommen, insofern der BND die NSA-Selektoren teils nicht überprüfte, teils bestehende Bedenken über problematische Ziele nicht an die zuständige Aufsicht im Kanzleramt weitergab.

Im Zuge der neuen Aufmerksamkeit für Selektoren wird außerdem bekannt, dass der BND selbst ebenfalls unerlaubte Ziele anvisiert (Götschenberg 2015; Spiegel Online 2015). Eine Reaktion auf diese neue Irritation ist eine Initiative aus der Welt der Opposition, den formalen Untersuchungsauftrag des NSAUA zu erweitern (Biermann 2016b). Der Vorschlag ist, der BND selbst solle auch direkt Gegenstand des NSAUA werden, anstatt wie bisher nur im Rahmen seiner Beteiligung an ausländischen Operationen Thema sein zu dürfen. Dafür legen Abgeordnete der Oppositionsfraktionen einen Antrag vor, der die Erweiterung regeln soll (Deutscher Bundestag 2016c; Biselli 2016a). Ähnlich wie bei der Einsetzung des NSAUA wird der Oppositionsantrag nicht ohne Änderungen vom Parlament angenommen. Stattdessen wird vier Monate lang in einem vermittelnden Ausschuss verhandelt. Ergebnis ist ein Kompromiss (Deutscher Bundestag 2016d): Zwar darf der NSAUA BND-Selektoren untersuchen, allerdings nur solche, die vom BND als problematisch entfernt wurden.

So hat sich der formale Teil der NSAUA-Arena erfolgreich selbst transformiert und auf eine Verschiebung des Issues reagiert bzw. diese Verschiebung weitergetrieben. Das Ausmaß der Erweiterung allerdings ist gering, etwa im Vergleich mit dem ursprünglichen Vorschlag der Oppositionsfraktionen. Es ist vor allem die Welt der Regierung und ihr Einfluss auf die Welt des Parlaments, die eine Verschiebung und Ausweitung des NSAUA-Issue hemmen. Vermutlich haben Regierungsvertreter*innen den vermittelnden Ausschuss besucht, um die Handlungsfähigkeit der Nachrichtendienste gegenüber dem Oppositionsvorschlag zu verteidigen (Biselli 2016b). Auch den teilweise dokumentierten Verhandlungen im vermittelnden Ausschuss lässt sich entnehmen, dass es von Seiten der Koalitionsfraktionen Bedenken gegenüber der Erweiterung gab. Diese beziehen sich im Sinne der Regierung auch auf den Schutz der Gewaltenteilung und das Staatswohl, also auf Konzepte, die den Arkanbereich der Regierung stärken (Deutscher Bundestag 2016d: 6). Darüber hinaus haben die Abgeordneten der Koalitionsfraktionen bei der Abstimmung im Bundestag nicht für eine Erweiterung gestimmt und sich stattdessen enthalten (Deutscher Bundestag 2016b: 17353).

9. SITZUNG:
Die Souveränität Deutschlands ist eine Illusion

2. SITZUNG
Streit im NSA-Ausschuss über Befragung Snowdens

1. SITZUNG
NSA-Ausschuss nimmt seine Arbeit auf

Maßnahmen der NSA unvereinbar mit Menschenrecht und Datenschutz

5. SITZUNG
Praktiken des BND möglicherweise rechtswidrig

8. SITZUNG
Ausschuss will Snowden per Videoübertragung vernehmen

7. SITZUNG
Snowden soll als Zeuge in den Ausschuss kommen

11. SITZUNG
Tiefste Bedrohung der Demokratie seit US-Bürgerkrieg

14. SITZUNG
Was machen NSA und BND zusammen in Bad Aibling?

12. SITZUNG
Nichtöffentliche Beratungssitzung

Donnerstag, 25. September 2014

NSA_UA

3.5 Reform durch Legalisierung?

Zum Zeitpunkt der vorliegenden Untersuchung ist die Arbeit des NSAUA nicht abgeschlossen. Aussagen über endgültige Effekte sind schon deshalb nicht möglich. Beobachtbar sind aber von der Bundesregierung angestoßene und am 21.10.2016 mit den Stimmen der Koalitionsparteien beschlossene Gesetzesänderungen, welche die Befugnisse des BND neu regeln (Bundesregierung 2016; Deutscher Bundestag 2016e). Die Welt der Regierung und Teile der Parlamentswelt loben die Änderung als Präzisierung der Rechtslage und Stärkung der Kontrolle der Nachrichtendienste (Bundesregierung 2016; Deutscher Bundestag 2016f: 18274 – 1875, 18277 – 18279, 18280 – 18283). Die Welten der Opposition (Deutscher Bundestag 2016f: 18276 – 18277, 18279 – 18280), der Nachrichten (Biermann 2016e; Deutscher Journalisten-Verbund 2016), der Netzgemeinde (Meister 2016b; Tripp 2016), der Rechtsanwendung (Papier 2016; Huber 2016) sowie internationale Menschenrechtsorganisationen (Amnesty International 2016; Reporter ohne Grenzen 2016b; Humanistische Union 2016) lehnen die neuen Gesetze als kontraproduktiv ab. Auch im Rahmen einer Sachverständigenanhörung im Innenausschuss des Bundestages werden die Änderung kontrovers diskutiert (Deutscher Bundestag 2016g).

Die gesetzlichen Neuregelungen können als Reaktion auf die Arbeit des NSAUA und als ihr vorläufiges Ergebnis verstanden werden, auch wenn der Abschlussbericht des NSAUA zum Zeitpunkt der Verabschiedung nicht vorliegt.[33] Die Gesetzesänderungen adressieren mithin jene Probleme, die durch die Arbeit des NSAUA registriert und verhandelt werden. Die Neuerungen sind damit eine Manifestation der produktiven Arbeit am Issue in der NSAUA-Arena. Fragwürdig bleibt jedoch die Nachhaltigkeit des beschrittenen Lösungswegs. Denn die Änderungen zielen weniger darauf ab, die in der Arena als problematisch registrierten Praktiken zukünftig institutionell auszuschließen. Der Lösungsansatz besteht vielmehr darin, jene Routinen durch Änderungen der Rechtsordnung gegen künftige Problematisierungen zu immunisieren und damit letztendlich zu stabilisieren.[34]

Zusammenfassend und mit Blick auf die in diesem Kapitel analysierten Ereignisse kann ich festhalten, dass die Art und Weise der Problembearbeitung in der NSAUA-Arena eine oszillierende Bewegung zwischen zwei Polen beschreibt: Einerseits werden in Reaktion auf Snowden mit der Entscheidung für einen

33 „Heute wollen wir aus der Aufklärungsarbeit im NSA-Untersuchungsausschuss und auch im Parlamentarischen Kontrollgremium unsere Konsequenzen ziehen und die weitreichendste Reform des BND-Gesetzes seit Jahrzehnten beschließen Mit den heute verabschiedeten Gesetzen stärken wir die parlamentarische Kontrolle, wir verbessern die Regierungsaufsicht, und wir sorgen für mehr Rechtssicherheit für den BND; denn Rechtssicherheit und Kontrolle schaffen auch Vertrauen" (Deutscher Bundestag 2016h: 19634).

34 Geschichtswissenschaftler Josef Foschepoth: „Historisch betrachtet sind alle größeren Geheimdienstaffären in der Bundesrepublik zugunsten der Dienste ausgegangen" (Krempl 2016).

Untersuchungsausschuss Routinen aktiviert, die eine reflexive Transformation demokratischer Institutionen anstoßen können. Andererseits lenken einige der frühen Entscheidungen die gemeinsame Arbeit gerade nicht auf Routinen der deutschen Demokratie, sondern viel mehr auf Probleme außerhalb der eigenen Ordnung. Doch trotz dieser ursprünglichen Ausrichtung auf externe Akteur*innen (NSA) verschiebt sich die Aufmerksamkeit in der Arena im Laufe der Arbeit auf inländische Institutionen (BND). In Folge wird eine formale Erweiterung des NSAUA angestoßen, die dann allerdings nur bruchstückhaft umgesetzt werden kann. Auch hier zeigt sich, dass die Arena eine reflexive Selbsttransformation nicht ausschließt, diese jedoch in engen Grenzen hält. Vorläufige Folgen der Arbeit in der NSAUA-Arena sind umstrittene Gesetzesänderungen zur Neureglung der Befugnisse des BND. Diese scheinen weniger auf eine Veränderung interner Routinen abzuzielen und stattdessen auf deren Stabilisierung durch eine entsprechende Anpassung der Rechtslage. Die Arena beweist an dieser Stelle mehr Beharrungsgeschick als die Fähigkeit zur Selbstransformation.

Im nächsten und abschließenden Kapitel werde ich die Oszillation des Issues und seiner Bearbeitung als Ergebnis des Zusammenspiels zweier Modi demokratischer Politik beschreiben. Dieser Interpretation nach vollziehen sich die Problembearbeitungen in der NSAUA-Arena in einem Spannungsfeld zwischen zwei spezifischen Reaktionsformen der Demokratie, die sich zugleich stützen und blockieren. Es ist diese Konstellation demokratischer Politiken, die die Grenzen der Issue-Oszillation beschreibt und ihre Amplituden in der NSAUA-Arena definiert.

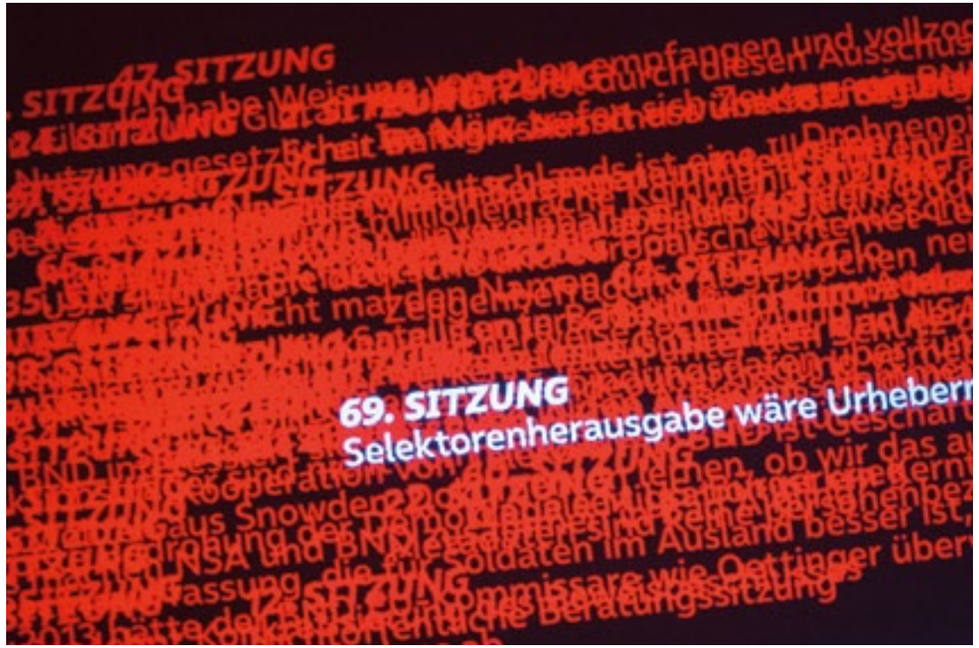
4. Welche Demokratie? Welche Privatheit?

4.1 Demokratie und Privatheit

Im letzten Kapitel kann ich zusammenfassend festhalten, welche Formen demokratischer Politik in der Arena mobilisiert werden und wie dabei die Krise der Privatheit bearbeitet wird. Privatheit und Demokratie zusammenzudenken ist keine ungewöhnliche Position; im Gegenteil finden sich zahlreiche Veröffentlichungen, die (eine bestimmte Form von) Privatheit als notwendige Voraussetzung für (eine bestimmte Form von) Demokratie verstehen (z.B. Westin 1967; Rössler 2001; Seubert 2012). Ich gehe außerdem davon aus, dass der Zusammenhang zwischen Demokratie und Privatheit nicht

nur in eine Richtung verläuft: Wenn Privatheit als Komponente von Demokratie zu verstehen ist, kann eine Neuordnung des Privaten auch mit einem Wandel der Demokratie einhergehen (Büttner et al. 2016). Jede politische Verhandlung von Privatheit kann immer auch eine Reproduktion oder Modifikation demokratischer Politik bedeuten. Damit können weder Demokratie noch Privatheit als feste Größen gefasst werden, sondern nur als bewegliche Variablen, die teils in Abhängigkeit voneinander restabilisiert oder transformiert werden.

In diesem Sinne ist es ratsam, in einer Kontroverse um die Zukunft der Privatheit nach den diversen Artikulationen der Demokratie zu suchen, um dann vor diesem Hintergrund nach den potenziell multiplen Formen des Privaten in der Kontroverse zu forschen. Wie im ersten Kapitel beschrieben, verstehe ich die NSAUA-Arena als ein Segment der Kontroverse um das Issue Privatheit. Die kollektive Arbeit am Issue des NSAUA ist deshalb auch Arbeit in der Privacy-Arena und am Issue Privatheit: Erstens direkt, insofern die Bedrohung oder der Schutz von Privatheit explizit Teil des Problems der Ausschussarbeit sind, und zweitens indirekt, insofern in der NSAUA-Arena immer auch über die Zukunft demokratischer Politik in Zeiten der Digitalisierung verhandelt wird, was wiederum (hemmend oder beschleunigend) an der Transformation des Privaten mitwirkt. Praktisch sind diese beiden Komplexe eng miteinander verwoben: Die Demokratieformen der Arena beeinflussen, wie das Issue Privatheit erfasst wird und welche Lösungsansätze in Frage kommen, während umgekehrt diverse Konzeptionen von Privatheit auf bestimmte Demokratiemodi stabilisierend und auf andere transformierend wirken.



4.2 Amplituden des Issues: Protektionismus und Konstitutionalismus

Vor dem Hintergrund der hier vorgestellten Kartografie der NSAUA-Arena zeigt sich die Kontroverse geprägt durch eine Konstellation aus zwei spezifischen Modi demokratischer Politik. Insbesondere die im Zuge diverser Zuschnitte und Transformationen nachvollzogenen Bewegungen des NSAUA-Issues lassen sich als Artikulationen dieser beiden Demokratiemodi lesen. Das Zusammenspiel der beiden Modi resultiert in einer Oszillation des Issues zwischen den Polen dieser idealtypischen Artikulationen der Demokratie (Lamla/Ochs 2017). Damit geht nicht zuletzt eine Begrenzung der kollektiven Suche nach Problemdefinitionen und entsprechenden Lösungen einher. Die Ausschläge und Amplituden der Problembearbeitung bleiben beschränkt auf das Feld zwischen diesen beiden Modi demokratischer Politik (Ochs/Pittroff/Büttner/Lamla 2016).

Den ersten Modus demokratischer Politik bezeichne ich hier als demokratischen Protektionismus (Lamla/Ochs 2017: 92f): Für diese Artikulationsweise der Demokratie ist es typisch, an Routinen festzuhalten. Bedrohungen und Probleme (für Privatheit oder Demokratie) werden außerhalb bewährter Routinen verortet und die eigenen Institutionen kaum in Frage gestellt. In der Öffentlichkeit wird zwar um Zustimmung gebeten, nicht aber um Beiträge oder Erweiterungen der Problemdefinition. Breite öffentliche Problemberatungen sind nicht vorgesehen. Stattdessen kümmern sich Eliten und Expert*innen aus Staat und Industrie um die Suche nach Lösungen. Passend dazu ist der demokratische Protektionismus gekennzeichnet durch Opazität: Probleme werden eher intransparent in repräsentativ-demokratischen Gremien oder Ministerien beraten.

Im NSAUA sind eine Reihe protektionistischer Praktiken und Diskurse zu beobachten. So wird etwa die Digitalisierung als Problem mit externen Ursachen behandelt, gegen das sich die deutsche Ordnung schützen muss (Deutscher Bundestag 2014b: 1816). Entsprechend wird insbesondere in der Anfangsphase des NSAUA versucht, die Ursache des Problems bei externen Akteur*innen wie der NSA zu verorten. Höhepunkt protektionistischer Politik in der Arena aber ist die beschlossene Änderung des BND-Gesetztes: Im Zentrum der Gesetzesänderung steht die Fortsetzung bestehender Routinen des BND. Darüber hinaus wurde das Gesetz kaum öffentlich beraten: Das Gesetz wurde genauso vom Bundestag verabschiedet, wie es das Bundeskanzleramt vorgeschlagen hat (Bundesregierung 2016; Deutscher Bundestag 2016i).

Den zweiten Demokratiemodus bezeichne ich als demokratischen Konstitutionalismus (Lamla/Ochs 2017: 93). Dieser Modus stützt sich auf abstrakte Prinzipien wie Verfassungsrecht oder Menschenrechte. Auf Basis solcher Konzepte werden interne Probleme thematisiert, ohne die Ordnung des Gemeinwesens insgesamt in Frage zu stellen. Der NSAUA und Untersuchungsausschüsse im Allgemeinen sind formal typische Erscheinungsformen eines demokratischen Konstitutionalismus; außerordentliche Routinen, um Missstände vor dem Hintergrund der Verfassung aufzudecken und zu reformieren. Doch trotz dieser formalen Anlage dominiert der Konstitutionalismus die NSAUA-Arena nicht.

Die Analyse der NSAUA-Arena verdeutlicht im Gegenteil die Grenzen des demokratischen Konstitutionalismus. Auf der einen Seite zeigen sich zwar immer wieder konstitutionalistische Momente in der Arena wie etwa die Verschiebung des Untersuchungschwerpunktes hin zu den internen Routinen deutscher Politik und die Selbsttransformation des Ausschusses durch eine Erweiterung seines Auftrages. Auf der anderen Seite bleiben die Routinen des NSAUA an die etablierten Institutionen des Nationalstaats gebunden und konstitutionalistische Politiken können sich nur eingeschränkt entfalten. Am Ende werden die reflexiven Problematisierungen des Ausschusses sogar als Input für protektionistische Reformen verwendet.

Diese Situation hat Folgen für die Rolle von Privatheit in der NSAUA-Arena. Abhängig davon, welche Politik im Ausschuss möglich ist, wird auch Privatheit auf verschiedenen Arten geschützt, kritisiert, instrumentalisiert oder verändert. Privatheit wird im Untersuchungsauftrag des NSAUA genannt und ist auch darüber hinaus Teil der Aushandlungen in der Arena (Deutscher Bundestag 2014a). Doch im limitierten Spannungsfeld zwischen Protektionismus und Konstitutionalismus erscheint Privatheit stets als stabiler Wert. So wird Privatheit immer nur geschützt – entweder protektionistisch in Kontrast zum Wert der Sicherheit oder konstitutionalistisch als bürger- oder menschenrechtliche Norm. Neue Formen von Privatheit und die Transformationspotenziale des Privaten finden in diesem Spektrum kaum Resonanz (Ochs 2015, 2017).

Zum Schluss lade ich dazu ein, die Beschäftigung mit der NSAUA-Arena über einen alternativen Zugang fortzusetzen. Im Rahmen unseres Projekts haben die Künstler*innen die dreijährigen Kontroversen des NSAUA zu einer 15-minütigen Video- und Sound-Installation komprimiert. Jeder Bassschlag dieser Sequenz repräsentiert eine der Sitzungen des Ausschusses, während langgezogene Töne den mäandernden Aufstieg und Fall widerstreitender Interessen nachzeichnen. In diesen trägen Fluss aus stetigem Rhythmus und langen Flächen brechen immer wieder zentrale Ereignisse in Form öffentlicher Aussagen ein, die die Ausschussarbeit verändert haben. Gleichzeitig erscheinen auf der Bildebene zentrale Zitate der Kontroverse, die eine Zeit lang als aktuell aufleuchten, bevor sie verblassen und mit den vorangegangenen Textstücken verschmelzen. Diese audiovisuelle Transformation der NSAUA-Arena macht die zähe, politische Oszillation der Kontroverse hör- und sehbar:
https://vimeo.com/219681007

LITERATUR

Amnesty International (2016): Privatsphäre ist ein Menschenrecht. https://www.amnesty.de/2016/9/2/privatsphaere-ist-ein-menschenrecht [zuletzt geprüft am 20.02.2017].
Baumgärtner, Maik/Gude, Hubert/Rosenbach, Marcel/Schindler, Jörg (2015): Neue Spionageaffäre erschüttert BND. http://www.spiegel.de/politik/deutschland/ueberwachung-neue-spionageaffaere-erschuettert-bnd-a-1030191.html [zuletzt geprüft am 20.02.2017].
Biermann, Kai (2014a): Schüchtert der Bundestag Medien ein? http://www.zeit.de/politik/deutschland/2014-10/bnd-nsa-ausschuss-netzpolitik-blog/komplettansicht [zuletzt geprüft am 20.02.2017].
Biermann, Kai (2014b): BND schickte wissentlich Daten von Deutschen an die NSA. http://www.zeit.de/digital/datenschutz/2014-10/bnd-nsa-de-cix-datenschutz-eikonal [zuletzt geprüft am 20.02.2017].
Biermann, Kai (2015a): Der Geheimhalter. http://www.zeit.de/politik/deutschland/2015-11/nsa-bnd-nsaua-geheimdienst-ausschuss-wolff/komplettansicht [zuletzt geprüft am 20.02.2017].
Biermann, Kai (2015b): BND-Chef Schindler will nichts gewusst haben. http://www.zeit.de/politik/deutschland/2015-05/schindler-bnd-nsa-untersuchungsausschuss [zuletzt geprüft am 20.02.2017].
Biermann, Kai (2015c): Der BND, ein gefährlicher Staat im Staat. http://www.zeit.de/politik/deutschland/2015-04/spionage-bnd-nsa-selektoren-spionage-europa [zuletzt geprüft am 20.02.2017].
Biermann, Kai (2016a): Geheim, weil peinlich? http://www.zeit.de/politik/deutschland/2016-07/nsa-bnd-spionage-gutachten-datenschutz/komplettansicht [zuletzt geprüft am 20.02.2017].
Biermann, Kai (2016b): Opposition will sich den BND vorknöpfen. http://www.zeit.de/politik/deutschland/2016-02/ueberwachung-bnd-untersuchung-opposition/komplettansicht [zuletzt geprüft am 20.02.2017].
Biermann, Kai (2016c): Der Teflon-Zeuge. http://www.zeit.de/politik/2016-03/nsa-affaere-frank-walter-steinmeier-untersuchungsausschuss/komplettansicht [zuletzt geprüft am 20.02.2017].
Biermann, Kai (2016d): Ist Maaßen ein russischer Agent? http://www.zeit.de/politik/deutschland/2016-06/edward-snowden-maassen-verfassungsschutz-nsaua/komplettansicht [zuletzt geprüft am 20.02.2017].
Biermann, Kai (2016e): Voller Zugriff auf die Kabel der Telekom. http://www.zeit.de/digital/datenschutz/2016-06/bnd-bundesnachrichtendienst-gesetz-reform/komplettansicht [zuletzt geprüft am 20.02.2017].
Biermann, Kai (2017a): Kanzleramt erklärt NSA-Affäre endgültig für beendet. http://www.zeit.de/politik/deutschland/2017-02/nsa-skandal-angela-merkel-kanzleramt-bnd-geheimdienste/komplettansicht [zuletzt geprüft am 07.03.2017].
Biermann, Kai (2017b): Die letzte Zeugin. http://www.zeit.de/politik/deutschland/2017-02/nsa-untersuchungsausschuss-angela-merkel-datenspionage-aussage-bnd/komplettansicht [zuletzt geprüft am 07.03.2017].
Biermann, Kai/Beuth, Patrick (2015): Was sind eigentlich Selektoren? http://www.zeit.de/digital/datenschutz/2015-04/bundesnachrichtendienst-bnd-nsa-selektoren-eikonal [zuletzt geprüft am 20.02.2017].
Biermann, Kai/Beuth, Patrick/Steffen, Tilmann (2015): BND half NSA beim Überwachen europäischer Politiker. http://www.zeit.de/digital/datenschutz/2015-04/ueberwachung-bnd-half-nsa-wirtschaftsspionage-europa [zuletzt geprüft am 20.02.2017].
Biselli, Anna (2016a): NSA-Untersuchungsausschuss: Opposition stellt Antrag zur Erweiterung des Untersuchungsauftrages. https://netzpolitik.org/2016/nsa-untersuchungsausschuss-opposition-stellt-antrag-zur-erweiterung-des-untersuchungsauftrages/ [zuletzt geprüft am 20.02.2017].
Biselli, Anna (2016b): NSA-Untersuchungsausschuss: Erweiterung des Untersuchungsauftrages mit Kompromissen. https://netzpolitik.org/2016/nsa-untersuchungsausschuss-erweiterung-des-untersuchungsauftrages-mit-kompromissen/ [zuletzt geprüft am 20.02.2017].
Bundesregierung (2016): Klare Regeln für Auslandsaufklärung. https://www.bundesregierung.de/Content/DE/Artikel/2016/06/2016-06-28-gesetz-bnd-ausland-ausland-fernmeldeaufklaerung.html [zuletzt geprüft am 20.02.2017].
Büttner, Barbara/Geminn, Christian L./Hagendorff, Thilo/Pittroff, Fabian/Lamla, Jörn/Ledder, Simon/Ochs, Carsten (2016): Die Reterritorialisierung des Digitalen. Zur Reaktion nationaler Demokratie auf die Krise der Privatheit nach Snowden. Kassel: Kassel University Press.
Callon, Michel (1980): Struggles and Negotiations to Define What is Problematic and What is Not: The Sociologic Translation. In: Karin D. Knorr, Roger Krohn und Richard Whitley (Hg.): The Social Process of Scientific Investigation. Dordrecht, Boston, London: D. Reidel Publishing Company, S. 197 – 220.
Callon, Michel (2006): Einige Elemente einer Soziologie der Übersetzung: Die Domestikation der Kammmuscheln und der Fischer der St. Brieuc-Bucht. In: Andréa Belliger und David J. Krieger (Hg.): ANThology. Ein einführendes Handbuch zur Akteur-Netzwerk-Theorie. Bielefeld: Transcript, S. 135 – 174.
Chaos Computer Club e.V. (2016): Gutachten für NSA-BND-Untersuchungsausschuss: BND-Operationsgebiet Inland. http://www.ccc.de/de/updates/2016/operationsgebiet-inland [zuletzt geprüft am 20.02.2017].
Chaos Computer Club e.V. (o. J.): Hackerethik. https://www.ccc.de/en/hackerethik [zuletzt geprüft am 20.02.2017].
Clarke, Adele (2012): Situationsanalyse. Grounded Theory nach dem Postmodern Turn. Wiesbaden: Springer VS.
Clarke, Adele/Leigh Star, Susan (2007): The Social Worlds Framework: A Theory/Methods Package. In: Edward J. Hackett, Olga Amsterdamska, Michael Lynch und Judy Wajcman (Hg.): The Handbook of Science and Technology Studies. Cambridge, MA: MIT Press, S. 113 – 138.
Deutscher Bundestag (2009): Untersuchungsausschüsse. https://www.bundestag.de/blob/190568/ce3840e6f7dbfe7052aa62debf812326/untersuchungsausschuesse-data.pdf [zuletzt geprüft am 20.02.2017].
Deutscher Bundestag (2013a): Opposition fordert Aufklärung über Datenspionage. http://www.bundestag.de/dokumente/textarchiv/2013/45634153_kw26_de_internetueberwachung/213038 [zuletzt geprüft am 20.02.2017].
Deutscher Bundestag (2013b): „Der Untersuchungsausschuss kommt mit Sicherheit". https://www.bundestag.de/dokumente/textarchiv/2013/47926096_kw48_interview_stroebele/214076 [zuletzt geprüft am 20.02.2017].
Deutscher Bundestag (2013c): Einigkeit in der Kritik an der NSA-Abhörpraxis. https://www.bundestag.de/dokumente/textarchiv/2013/47804054_kw47_de_nsa/214020 [zuletzt geprüft am 20.02.2017].
Deutscher Bundestag (2014a): Drucksache 18/843. Einsetzung eines Untersuchungsausschusses. http://dip21.bundestag.de/dip21/btd/18/008/1800843.pdf [zuletzt geprüft am 20.02.2017].
Deutscher Bundestag (2014b): Plenarprotokoll 18/23. http://dipbt.bundestag.de/doc/btp/18/18023.pdf [zuletzt geprüft am 20.02.2017].
Deutscher Bundestag (2014c): Experten für proaktiven Schutz vor Cyberangriffen. http://www.bundestag.de/dokumente/textarchiv/2014/kw26_1ua_nsa/283442 [zuletzt geprüft am 20.02.2017].
Deutscher Bundestag (2014d): Papier: Staat muss die Grundrechte wahren. https://www.bundestag.de/dokumente/textarchiv/2014/nsa_untersuchungsausschuss/279296 [zuletzt geprüft am 20.02.2017].
Deutscher Bundestag (2014e): Zeuge: G-10-Daten werden streng kontrolliert. http://www.bundestag.de/dokumente/textarchiv/2014/kw48_pa_nsa/341248 [zuletzt geprüft am 20.02.2017].
Deutscher Bundestag (2014f): Protokoll Ausschusssitzung. https://www.bundestag.de/blob/372414/917a74849c1937c8a63686c87525de94/05-papier_hoffmann-riem_baecker_endgueltig--1--data.pdf [zuletzt geprüft am 20.02.2017].
Deutscher Bundestag (2014g): Plenarprotokoll 18/14. http://dip21.bundestag.de/dip21/btp/18/18014.pdf [zuletzt geprüft am 20.02.2017].
Deutscher Bundestag (2014h): Drucksache 18/ 420. Einsetzung eines Untersuchungsausschusses. http://dip21.bundestag.de/dip21/btd/18/004/1800420.

pdf [zuletzt geprüft am 20.02.2017].
Deutscher Bundestag (2014i): Drucksache 18/483. Einsetzung eines Untersuchungsausschusses NSA. http://dipbt.bundestag.de/dip21/btd/18/004/1800483.pdf [zuletzt geprüft am 20.02.2017].
Deutscher Bundestag (2014j): Keine Informationen an die NSA übermittelt. http://www.bundestag.de/dokumente/textarchiv/2014/kw46_pa_1ua/339510 [zuletzt geprüft am 20.02.2017].
Deutscher Bundestag (2014k): Plenarprotokoll 18/56. http://dip21.bundestag.de/dip21/btp/18/18056.pdf [zuletzt geprüft am 20.02.2017].
Deutscher Bundestag (2015a): Stenographisches Protokoll der 77. Sitzung. http://www.bundestag.de/blob/407450/439d2da82430a5e034176b6ca8cde609/77_2-a-sch_geschwaerzt-data.pdf [zuletzt geprüft am 20.02.2017].
Deutscher Bundestag (2015b): Protokoll 18/37. https://wikileaks.org/bnd-nsa/sitzungen/37/index.de.html [zuletzt geprüft am 20.02.2017].
Deutscher Bundestag (2016a): NSA-Ausschuss soll sich auch mit BND-Selektoren befassen. https://www.bundestag.de/presse/hib/201606/-/426804 [zuletzt geprüft am 20.02.2017].
Deutscher Bundestag (2016b): Drucksache 18/7565. http://dip21.bundestag.de/dip21/btd/18/075/1807565.pdf [zuletzt geprüft am 20.02.2017].
Deutscher Bundestag (2016c): Plenarprotokoll 18/176. http://dipbt.bundestag.de/doc/btp/18/18176.pdf [zuletzt geprüft am 20.02.2017].
Deutscher Bundestag (2016d): Drucksache 18/8683. http://dip21.bundestag.de/dip21/btd/18/086/1808683.pdf [zuletzt geprüft am 20.02.2017].
Deutscher Bundestag (2016e): Drucksache 18/10068. http://dip21.bundestag.de/dip21/btd/18/100/1810068.pdf [zuletzt geprüft am 20.02.2017].
Deutscher Bundestag (2016f): Plenarprotokoll 18/184. http://dipbt.bundestag.de/dip21/btp/18/18184.pdf [zuletzt geprüft am 20.02.2017].
Deutscher Bundestag (2016g): BND-Gesetzentwurf stößt auf kontroverse Bewertung. http://www.bundestag.de/dokumente/textarchiv/2016/kw39-pa-inneres/459384 [zuletzt geprüft am 20.02.2017].
Deutscher Bundestag (2016h): Plenarprotokoll 18/197. http://dip21.bundestag.de/dip21/btp/18/18197.pdf [zuletzt geprüft am 20.02.2017].
Deutscher Bundestag (2016i): Drucksache 18/9041. http://dip21.bundestag.de/dip21/btd/18/090/1809041.pdf [zuletzt geprüft am 20.02.2017].
Deutscher Bundestag (o. J. a): 1. Untersuchungsausschuss („NSA"). http://www.bundestag.de/ausschuesse18/ua/1untersuchungsausschuss [zuletzt geprüft am 20.02.2017].
Deutscher Bundestag (o. J. b): Gremien zur Kontrolle. https://www.bundestag.de/parlament/aufgaben/regierungskontrolle_neu/kontrolle/grem/255458 [zuletzt geprüft am 20.02.2017].
Deutscher Journalisten-Verbund (2016): Nein zur Journalisten-Hatz! https://www.djv.de/startseite/profil/der-djv/pressebereich-download/pressemitteilungen/detail/article/nein-zur-journalisten-hatz.html [zuletzt geprüft am 20.02.2017].
Digitalcourage (2014): Eine Million Aufkleber fordern Asyl für Edward Snowden. https://digitalcourage.de/blog/2014/eine-million-aufkleber-fordern-asyl-fuer-edward-snowden [zuletzt geprüft am 20.02.2017].
Dolderer, Winfried (2016): „Niemals näher als jetzt". http://www.das-parlament.de/2016/12_13/innenpolitik/-/415944 [zuletzt geprüft am 20.02.2017].
Fennen, Nicolas (2013): BND hat Zugriff auf deutschen Internetknoten DE-CIX. https://netzpolitik.org/2013/bnd-hat-zugriff-auf-deutschen-internetknoten-de-cix/ [zuletzt geprüft am 20.02.2017].
Geist, Anton/Gjerding, Sebastian/Moltke, Henrik/Poitras, Laura (2014): NSA 'third party' partners tap the Internet backbone in global surveillance program. https://www.information.dk/udland/2014/06/nsa-third-party-partners-tap-the-internet-backbone-in-global-surveillance-program [zuletzt geprüft am 20.02.2017].
Golem.de (o. J.): NSA -Untersuchungsausschuss. https://www.golem.de/specials/nsa-untersuchungsausschuss/ [zuletzt geprüft am 20.02.2017].
Götschenberg, Michael (2015): BND NSA-Untersuchungsausschuss-Geplaenkel-statt-Aufklaerung,nsa284.html [zuletzt geprüft am 20.02.2017].
Knorr, Karin D./Krohn, Roger/Whitley, Richard (Hg.) (1980): The Social Process of Scientific Investigation. Dordrecht, Boston, London: D. Reidel Publishing Company.
Krempl, Stefan (2016): BND-Reform: Bundesregierung befürwortet großflächige Internetüberwachung. https://www.heise.de/newsticker/meldung/BND-Reform-Bundesregierung-befuerwortet-grossflaechige-Internetueberwachung-3250327.html [zuletzt geprüft am 07.03.2017].
Kurz, Constanze (2016): Mein Name ist Hase, ich weiß von nichts. http://www.faz.net/aktuell/feuilleton/aus-dem-maschinenraum/steinmeier-im-nsa-untersuchungsausschuss-14136313.html?printPagedArticle=true#pageIndex_2 [zuletzt geprüft am 20.02.2017].
Lamla, Jörn (2013): Verbraucherdemokratie. Politische Soziologie der Konsumgesellschaft. Berlin: Suhrkamp.
Lamla, Jörn/Ochs, Carsten (2017): Der NSA-Skandal als Krise der Demokratie? Selbstreflexionen der Öffentlichkeit in der Privacy-Arena. In: Kornelia Hahn und Andreas Langenohl (Hg.): Kritische Öffentlichkeiten - Öffentlichkeiten in der Kritik. Wiesbaden: Springer VS, S. 83 – 112.
Latour, Bruno (2007): Turning Around Politics - A Note on Gerard de Vries' Paper. In: Social Studies of Science 37 (5), S. 811 – 820.
Latour, Bruno (2010): Das Parlament der Dinge. Für eine politische Ökologie. Frankfurt am Main: Suhrkamp.
Linksfraktion (2016): Opposition lässt nichts unversucht – Zeuge Snowden soll nach Deutschland. https://www.linksfraktion.de/presse/pressemitteilungen/detail/opposition-laesst-nichts-unversucht-zeuge-snowden-soll-nach-deutschland/ [zuletzt geprüft am 20.02.2017].
Lobo, Sascha (2012): Die Netzgemeinde ist eine Notwehr-Lobby. http://www.spiegel.de/netzwelt/web/s-p-o-n-die-mensch-maschine-die-netzgemeinde-ist-eine-notwehr-lobby-a-819559.html [zuletzt geprüft am 20.02.2017].
Lohse, Eckart (2016): Die NSA-Affäre als Karriere-Chance. http://www.faz.net/aktuell/politik/inland/patrick-sensburg-die-nsa-affaere-als-karriere-chance-13681574.html [zuletzt geprüft am 20.02.2017].
Marres, Noortje (2007): The issues deserve more credit. Pragmatist Contributions to the study of public involvement in controversy. In: Social Studies of Science 37 (5), S. 759 – 780.
Mascolo, Georg (2014): BND leitete Daten von Deutschen an NSA weiter. http://www.sueddeutsche.de/politik/spaeh-affaere-bnd-leitete-daten-vondeutschen-an-nsa-weiter-1.2157406 [zuletzt geprüft am 20.02.2017].
Mascolo, Georg/Leyendecker, Hans/Goetz, John (2014): Codewort Eikonal - der Albtraum der Bundesregierung. http://www.sueddeutsche.de/politik/geheimdienste-codewort-eikonal-der-albtraum-der-bundesregierung-1.2157432
hörte deutschen Diplomaten ab. https://www.tagesschau.de/inland/bnd-selektorenliste-103.html [zuletzt geprüft am 20.02.2017].
Grünenfraktion (2016): BND wird offiziell zur Massenüberwachungsmaschine. https://www.gruene-bundestag.de/presse/pressemitteilungen/2016/juni/bnd-wird-offiziell-zur-massenueberwachungsmaschine-28-06-2016.html [zuletzt geprüft am 20.02.2017].
Hayden, Michael (2016): „Wir sind perfekt. Nur die Einschätzungen zum Irak waren falsch, wirklich falsch". http://www.stern.de/politik/ausland/michael-hayden--ex-chef-von-nsa-und-cia---wir-haben-fehler-gemacht--6858586.html [zuletzt geprüft am 20.02.2017].
Huber, Bertold (2016): Geheimdienst-Kontrolleur: Neues BND-Gesetz wird sich „als evident verfassungswidrig erweisen". https://netzpolitik.org/2016/geheimdienst-kontrolleur-neues-bnd-gesetz-wird-sich-als-evident-verfassungswidrig-erweisen/ [zuletzt geprüft am 20.02.2017].
Humanistische Union (2016): Gesetzlich enthemmter Geheimdienst. http://www.humanistische-union.de/nc/aktuelles/aktuelles_detail/back/aktuelles/article/gesetzlich-enthemmter-geheimdienst/ [zuletzt geprüft am 20.02.2017].
Kempmann, Antonius/Pinkert, Reiko (2013): NSA-Untersuchungsausschuss: Geplänkel statt Aufklärung. http://daserste.ndr.de/panorama/aktuell/

[zuletzt geprüft am 20.02.2017].
Meister, Andre (2014a): Aussagegenehmigung: Wir veröffentlichen die Liste an Sachen, die BND-Mitarbeiter dem Parlament nicht sagen dürfen (Update). https://netzpolitik.org/2014/aussagegenehmigung-wir-veroeffentlichen-die-liste-an-sachen-die-bnd-mitarbeiter-dem-parlament-nicht-sagen-duerfen/ [zuletzt geprüft am 20.02.2017].
Meister, Andre (2014b): Live-Blog aus dem Geheimdienst-Untersuchungsausschuss: Sitzung nach wenigen Minuten abgebrochen. https://netzpolitik.org/2014/live-blog-aus-dem-geheimdienst-untersuchungsausschuss-bnd-abhoer-techniker-im-zeugenstand/ [zuletzt geprüft am 20.02.2017].
Meister, Andre (2016a): Geheimer Prüfbericht: Der BND bricht dutzendfach Gesetz und Verfassung – allein in Bad Aibling (Updates). https://netzpolitik.org/2016/geheimer-pruefbericht-der-bnd-bricht-dutzendfach-gesetz-und-verfassung-allein-in-bad-aibling/ [zuletzt geprüft am 20.02.2017].
Meister, Andre (2016b): Das neue BND-Gesetz: Alles, was der BND macht, wird einfach legalisiert. Und sogar noch ausgeweitet. https://netzpolitik.org/2016/das-neue-bnd-gesetz-alles-was-der-bnd-macht-wird-einfach-legalisiert-und-sogar-noch-ausgeweitet/ [zuletzt geprüft am 20.02.2017].
Meister, Andre (2017): Drei Jahre Geheimdienst-Untersuchungsausschuss:
Papier, Hans-Jürgen (2016): Beschränkungen der Telekommunikationsfreiheit durch den BND an Datenaustauschpunkten. In: Neue Zeitschrift für Verwaltungsrecht 35 (15), S. 1 – 15.
PUAG (2001): Gesetz zur Regelung des Rechts der Untersuchungsausschüsse des Deutschen Bundestages (Untersuchungsausschussgesetz - PUAG). http://www.gesetze-im-internet.de/bundesrecht/puag/gesamt.pdf [zuletzt geprüft am 20.02.2017].
Reporter ohne Grenzen (2016a): PETITION. https://www.reporter-ohne-grenzen.de/mitmachen/petition-bnd-en/ [zuletzt geprüft am 20.02.2017].
Reporter ohne Grenzen (2016b): Drei UN-Berichterstatter kritisieren BND-Reform. https://www.reporter-ohne-grenzen.de/presse/pressemitteilungen/meldung/drei-un-berichterstatter-kritisieren-bnd-reform/ [zuletzt geprüft am 20.02.2017].
Rössler, Beate (2001): Der Wert des Privaten. Frankfurt am Main: Suhrkamp.
Rössler, Beate (2016): Wie wir uns regieren. Soziale Dimensionen des Privaten in der Post-Snowden-Ära. In: WestEnd. Neue Zeitschrift für Sozialforschung 13 (1), S. 103 – 118.
Seemann, Michael (2011): Das politische Denken der Piraten. http://www.ctrl-verlust.net/das-politische-denken-der-piraten/ [zuletzt geprüft am 20.02.2017].
Seemann, Michael (2013): Netzgemeinde. http://mspr0.de/?p=3723 [zuletzt geprüft am 20.02.2017].
com-20090101-141017-99-06967 [zuletzt geprüft am 20.02.2017].
Süddeutsche.de (2014b): So biegt sich der BND das Recht zurecht. http://www.sueddeutsche.de/politik/nsa-ausschuss-so-biegt-sich-der-bnd-das-recht-zu-recht-1.2242129 [zuletzt geprüft am 20.02.2017].
Süddeutsche.de (o. J.): NSA-Ausschuss. http://www.sueddeutsche.de/thema/NSA-Ausschuss [zuletzt geprüft am 20.02.2017].
Tagesschau.de (2016): „Systematische Gesetzesverstöße" des BND. http://www.tagesschau.de/inland/bnd-315.html [zuletzt geprüft am 20.02.2017].
Technische Aufklärung (2015): TA001 – Was macht eigentlich der deutsche Geheimdienst-Untersuchungsausschuss. https://technische-aufklaerung.de/ta001-was-macht-eigentlich-der-deutsche-geheimdienst-untersuchungsausschuss/ [zuletzt geprüft am 20.02.2017].
Tripp, Volker (2016): BND-Reform verhindern: Telefonaktion und Petition gegen Massenüberwachung. https://digitalegesellschaft.de/2016/09/bnd-reform-verhindern/ [zuletzt geprüft am 20.02.2017].
Venturini, Tommaso (2010): Diving in magma: how to explore controversies with actor-network theory. In: Public Understandings of Science 19 (3), S. 258 – 273.
Westin, Alan F. (1967): Privacy and Freedom. New York.
Wikileaks.org (2015a): NSA Untersuchungsausschuss. https://wikileaks.org/bnd-

Die Aufklärung bleibt Wunschdenken, die Überwachung geht weiter. https://netzpolitik.org/2017/kommentar-zum-geheimdienst-untersuchungsausschuss-doch-nur-ein-ritual-das-die-illusion-einer-untersuchung-erwecken-soll/ [zuletzt geprüft am 07.03.2017].
Netzpolitik.org (2015): Live-Blog aus dem Geheimdienst-Untersuchungsausschuss: „Jeden Tag eine halbe Million Telefonate mitgeschnitten.". https://netzpolitik.org/2015/live-blog-aus-dem-geheimdienst-untersuchungsausschuss-37-sitzung-mit-e-b-und-r-s-vom-bnd-schoeningen/#zeuge1 [zuletzt geprüft am 20.02.2017].
Netzpolitik.org (o. J.): NSAUA-Liveblog. https://netzpolitik.org/tag/nsaua-liveblog/ [zuletzt geprüft am 20.02.2017].
Notz, Konstantin von (2015): Zum Abschuss freigegeben. http://www.spiegel.de/netzwelt/web/nsa-untersuchungsausschuss-zwischenbilanz-von-konstantin-von-notz-a-1024274.html [zuletzt geprüft am 20.02.2017].
Ochs, Carsten (2015): Die Kontrolle ist tot – lang lebe die Kontrolle! Plädoyer für ein nach-bürgerliches Privatheitsverständnis. In: www.medialekontrolle.de 4 (1). http://www.medialekontrolle.de/wp-content/uploads/2015/11/Ochs-Carsten-2015-04-01.pdf [zuletzt geprüft am 20.02.2017].
Ochs, Carsten/Pittroff, Fabian/Büttner, Barbara/Lamla, Jörn (2016): Governing the internet in the privacy arena. In: Internet Policy Review 5 (3).
Sensburg, Patrick (2015): Sensburg: BND hat EU-Ziele nicht rausgehalten. https://www.bundestag.de/dokumente/textarchiv/2015/kw29_interview_sensburg/382788 [zuletzt geprüft am 20.02.2017].
Seubert, Sandra (2012): Der gesellschaftliche Wert des Privaten. In: DuD - Datenschutz und Datensicherheit 36 (2), S. 100 – 104. DOI: 10.1007/s11623-012-0025-6.
Snowden, Edward (2014): ohne Titel. http://www.europarl.europa.eu/document/activities/cont/201403/20140307ATT80674/20140307ATT80674EN.pdf [zuletzt geprüft am 20.02.2017].
Spiegel Online (2015): BND spionierte Ministerien befreundeter Staaten aus. http://www.spiegel.de/politik/deutschland/bundesnachrichtendienst-spionierte-systematisch-freunde-aus-a-1061517.html [zuletzt geprüft am 20.02.2017].
Strauss, Anselm (1978): A Social World Perspective. In: Studies in Symbolic Interaction 1 (1), S. 119 – 128.
Strauss, Anselm (1982): Social Worlds and Legitimization Processes. In: Studies in Symbolic Interaction 4 (4), S. 171 – 190.
Strauss, Anselm (1993): Continual Permutations of Action. Hawthorne, NY: Aldine de Gruyter.
Süddeutsche.de (2014a): Blog «Netzpolitik» verfolgt NSA-Untersuchungsausschuss. http://www.sueddeutsche.de/news/wirtschaft/internet-blog-netzpolitik-verfolgt-nsa-untersuchungsausschuss-dpa.urn-newsml-dpa-nsa/sitzungen/37/index.de.html [zuletzt geprüft am 20.02.2017].
Wikileaks.org (2015b): NSA Untersuchungsausschuss. https://wikileaks.org/bnd-nsa/press/index.de.html [zuletzt geprüft am 20.02.2017].
Wikileaks.org (2015c): Bundestag Inquiry into BND and NSA. https://wikileaks.org/bnd-nsa/sitzungen/18/ [zuletzt geprüft am 20.02.2017].
Wissenschaftliche Dienste des Deutschen Bundestags (2006): Der Kernbereich exekutiver Eigenverantwortung. https://www.bundestag.de/blob/412760/1e98af44462dee55fd1ee3925501dbf4/wd-3-383-06-pdf-data.pdf [zuletzt geprüft am 20.02.2017].
Zeit Online (2014): Kanzleramt droht NSA-Ausschuss mit Strafanzeige. http://www.zeit.de/politik/deutschland/2014-10/kanzleramt-drohung-strafanzeige-nsa-untersuchungsausschuss [zuletzt geprüft am 20.02.2017].
Zeit Online (2016): Maaßen beklagt sich über NSA-Untersuchungsausschuss. http://www.zeit.de/digital/datenschutz/2016-06/nsa-untersuchungsausschuss-hans-georg-maassen-verfassungsschutz-edward-snowden-kritik [zuletzt geprüft am 20.02.2017].
Zeit Online (o. J.): Spionage in Deutschland. http://www.zeit.de/thema/nsa-affaere [zuletzt geprüft am 20.02.2017].

Big Data

von Andreas Baur-Ahrens,
Thilo Hagendorff, Maria Pawelec

05

Das ‚Große' an Big Data ist v.a. die Fähigkeit, die Masse an gesammelten Daten in Beziehung zu setzen, zeitnah zu verarbeiten und daraus durch geeignete Algorithmen Muster zu detektieren und neue Erkenntnisse zu gewinnen.

Boyd, Danah and Crawford, Kate (2012): Critical Questions for Big Data: Provocations for a cultural, technological, and scholarly phenomenon. In: Information, Communication & Society 15(5), S. 663.

Big Data ist einer der zentralen Streitgegenstände in der Privacy Arena, um den sich auf diversen Schauplätzen in der Arena (wie beispielsweise den Verhandlungen um die Datenschutz-Grundverordnung) verschiedene soziale Welten und deren Vertreter*innen versammeln, um dessen Zukunft zu verhandeln. Mit dem Begriff „Big Data" werden sehr große Datenmengen sowie neue Formen komplexer Datenverarbeitungsmethoden bezeichnet. Dabei geht es vor allem um die Erhebung und Verarbeitung personenbezogener Daten. Die Informationen, Muster und statistischen Regelmäßigkeiten, welche qua Data-Mining aus Datenbanken gezogen werden, betreffen jedoch nicht nur diejenigen Personen, deren Daten in den Datenbanken enthalten sind, sondern auch nicht „erfasste" Personen. Nicht zuletzt deswegen wird Big Data häufig in einem Atemzug genannt mit der Verletzung der Privatheit. Während Vertreter des Datenschutzes sich daher häufig gegen verschiedene Methoden von Big-Data-Analysen wenden, treten insbesondere Wirtschaftsvertreter dafür ein, Big Data zu nutzen, da die Datenanalysen für Unternehmen gewinnbringend eingesetzt werden können. Der Konflikt zwischen Wirtschaft, Datenschutz, Politik, Computerwissenschaft und Netzgemeinde erzeugt hier ein großes „Stimmengewirr", welches in der Kunstausstellung durch ein Zusammenschnitt aus data-data-data-Zitaten eingefangen wurde. Big Data geht einher mit einem Wirrwarr an Ideen und Anwendungsmöglichkeiten, Hoffnungen und Kritik – einem Hype, einem regelrechten „Datenrausch".

1. Was bedeutet Big Data?

Mit Big Data werden häufig nicht einfach nur große Datenmengen und Datenverarbeitungskonzepte bezeichnet, sondern eine neue Qualität der Datenverarbeitung und des Einflusses von Daten auf soziale Prozesse. Mit dem Konzept der Big Data soll die immer umfassendere Computerisierung und Verdatung der Welt gefasst werden. Dabei bezeichnet der Begriff nicht allein ein technologisches, sondern gleichsam ein kulturelles Phänomen (Byod & Crawford 2012). Es basiert auf dem „computational turn", welcher sich in so gut wie jedem sozialen Feld abzeichnet: Computertechnologien wirken zusammen, bestärken sich und können immer größere, dynamische, sich verändernde sowie sowohl strukturierte als auch unstrukturierte Datenmengen in immer größerer Geschwindigkeit speichern, prozessieren, analysieren und verbreiten (Kitchin 2014a). Dabei umfasst Big Data beispielsweise personenbezogene Verhaltensdaten, Daten aus sozialen Netzwerken, Daten über persönliche Interessen und Einstellungen, demografische Daten, Standortdaten, Daten über Transaktionen und Kaufverhalten und vieles mehr.

Big Data bezeichnet deshalb zwar auch das Erfassen und Sammeln großer Mengen verschiedenster und möglichst umfassender (auch auf den ersten Blick unwichtig erscheinender) Daten und dies am besten in Echtzeit (Kitchin 2014b). Big Data ist jedoch nicht nur gekennzeichnet durch das Sammeln und die Vermischung und damit die Menge an Daten allein, die durch immer mehr Sensoren und datenbasierte Interaktionen anfallen. Entscheidend ist auch die durch technischen Fortschritt geschaffene Möglichkeit, diese Datenberge zu durchsuchen, Muster zu erkennen und zu analysieren. Das „Große" an Big Data ist daher v.a. die Fähigkeit,

die Masse an gesammelten Daten zu speichern, in Beziehung zu setzen, zeitnah zu verarbeiten und daraus durch geeignete Algorithmen Muster zu finden und neue Erkenntnisse zu gewinnen (Boyd & Crawford 2012).

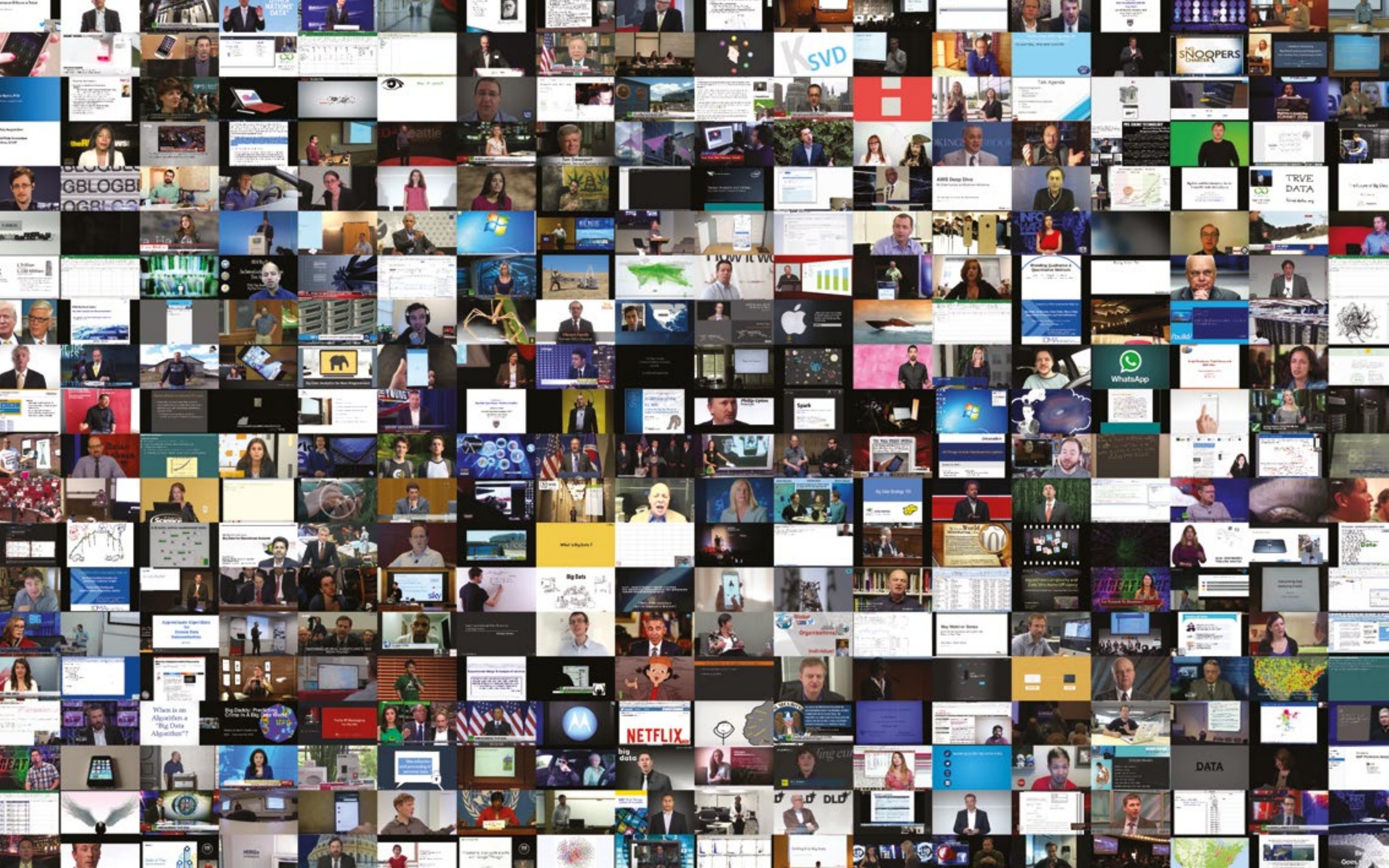
Big Data weckt Vorstellungen über den „mythischen" Charakter großer Datenmengen, aus denen Erkenntnisse über Sachverhalte und Ereigniszusammenhänge gewonnen werden können, die bis dato undenkbar waren. In diesem Zusammenhang werden über Big Data von manchen Akteuren sowohl soziotechnische Utopien einer smarten, nachhaltigen und hypereffizienten Informationsgesellschaft (Helbing et al. 2015) als auch Dystopien einer totalen Überwachungsgesellschaft gezeichnet (Welzer 2016). Daneben gibt es Positionen und Einschätzungen zu Big Data, die versuchen, den Problemgegenstand in seinem Ausmaß erst greifbar zu machen. Diese werden in den weiteren Unterpunkten dargestellt. Hierzu gehören der positive Fortschrittsglaube in Wissenschaft und Wirtschaft, aber auch die kritischen Stimmen aus der Algorithmenethik, die problematische Folgen von Big Data beleuchtet, sowie die Schwierigkeiten, diesen Folgen zu begegnen.

"Mit Big Data werden revolutionierende Umschwünge in der Wissenschaft, der Wirtschaft, dem Gesundheits- oder Polizeiwesen, der Politik und der persönlichen Lebenswelt sowie in vielen weiteren gesellschaftlichen Feldern verbunden."

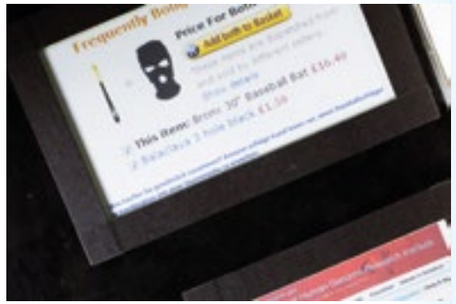
2. Fortschrittsversprechen von Big Data

Mit Big Data werden revolutionierende Umschwünge in der Wissenschaft, der Wirtschaft, dem Gesundheits- oder Polizeiwesen, der Politik und der persönlichen Lebenswelt sowie in vielen weiteren gesellschaftlichen Feldern erwartet und verbunden (Boyd Crawford 2012; Burkhardt 2015; Kitchin 2014b; Manovich 2014; Mayer-Schönberger & Cukier 2013; Reichert 2014; Vayena et al. 2015). In der sozialen Welt der Wissenschaft wird Big Data nicht nur in eine Reihe gestellt mit Paradigmen wie etwa der Kybernetik, der Gentechnologie oder den Neurowissenschaften, mit denen eine Art universelle Erklärungsallmacht assoziiert wird, sondern gleichzeitig in Zusammenhang mit einem „Ende der Theorie", welches durch die vermeintliche Selbstaussagekraft der Daten zustande kommt (Anderson 2008). Ähnlich hochgegriffene Potenziale verspricht man sich von Big Data in der Wirtschaftswelt, in welcher neue Formen der Marktforschung, der Vertriebs- und Servicesteuerung, der Werbung oder der Mitarbeiterauswahl etabliert werden könnten. In der Medizin sollen neue Methoden des digitalisierten Gesundheitswesens Krankheiten vor allem über Korrelationen zwischen Verhaltensweisen und deren gesundheitlichen Auswirkungen erklären. Im Polizeiwesen schließlich entsteht mit dem Predictive Policing (vorhersagende Polizeiarbeit) ein neuer methodischer Ansatz der vorhersehenden Kriminalitätsbekämpfung, welcher andere bürgernähere Ansätze wie etwa das Community Policing oder das Problem-Oriented Policing ergänzt bzw. ablöst. Auch in der Politik können Entscheidungen zunehmend auf der Grundlage von Erkenntnissen aus Big-Data-Analysen getroffen werden. Dies führt zu spezifischen Legitimationsproblemen, da dadurch statt Personen des politischen Systems prinzipiell intransparente Computersysteme zu Entscheidungsträgern werden. Schließlich beeinflusst Big Data auf vielfältige Weise auch die persönliche Lebenswelt der Nutzer*innen informationstechnischer Systeme, etwa, wenn über Big-Data-Analysen die Personalisierung von Diensten und Plattformen vorangetrieben und verfeinert wird. Dadurch werden immer personalisiertere Ergebnisse bei Suchmaschinen oder Werbeanzeigen, passende Musik- oder Filmempfehlungen, Kaufangebote oder auch Partnervorschläge bei der Online-Partnersuche angezeigt.

Diese Beispiele bilden nur einen kleinen Ausschnitt aus den potentiellen Auswirkungen und Einflüssen von Big Data auf die Informationsgesellschaft. Möglich werden diese Auswirkungen und Einflüsse, grob gesprochen, aus der aktuellen Technikentwicklung, aus der Ubiquität der Erhebung, Verarbeitung und Verbreitung großer Datenmengen. Big Data umfasst beispielsweise personenbezogene Verhaltensdaten, Daten aus sozialen Netzwerken, Daten über persönliche Interessen und Einstellungen, demografische Daten, Standortdaten, Daten über Transaktionen und Kaufverhalten und vieles mehr. Big Data steht aber nicht nur als Bezeichnung für jene großen Datenmengen, sondern meint immer auch eine Auswertung dieser Daten – mitunter auch als „data mining" oder „knowledge discovery in databases" (Wissensentdeckung in Datenbanken) bezeichnet (Vedder 1999). Dabei besteht ein wesentliches Ziel der Datenauswertung darin, Muster und Korrelationen in Datenbanken zu erkennen, um dadurch Wahrscheinlichkeitsprognosen für zukünftige Ereignisse oder unbekannte Merkmale zu tätigen. Dadurch wiederum kann etwa die situationsbezogene Assistenzleistung digitaler Medien in verschiedensten Lebensbereichen gesteigert sowie deren Funktion als Ergänzung und Erweiterung körperlicher und geistiger Fähigkeiten ausgebaut werden.


KSVD
SNOOPERS
TRVE DATA
WhatsApp
NETFLIX
DATA

Beispiel: Big Data als Zukunftsthema der Informationswirtschaft
Zum Themenfeld Big Data veröffentlichte eco, der Verband der Internetwirtschaft, bislang nur Stellungnahmen, welche die Chancen von Big Data für Marketing oder Mobilität hervorheben oder sich mit den technischen Herausforderungen beschäftigen. Privatheit und Risiken durch Big-Data-Anwendungen werden hingegen nicht thematisiert. Im Vorfeld der Finalisierung der Europäischen Datenschutz-Grundverordnung 2015 wandte sich hingegen der Bitkom, ein deutscher Industrieverband, der 2300 Unternehmen aus dem Bereich der digitalen Wirtschaft vertritt, mit Stellungnahmen und konkreten Formulierungsvorschlägen an die Bundesregierung, um die Interessen ihrer Mitglieder im Gesetzesvorhaben berücksichtigt zu sehen. Dem Bitkom zufolge solle das Hauptziel der Neuregelung des Datenschutzes in der EU im Hinblick auf die zunehmende Bedeutung von Big-Data-Anwendungen sein, „den europäischen Unternehmen zu ermöglichen, neue Technologien einzusetzen und innovative Datenverarbeitungen zu entwickeln“ (Bitkom 2015a). Der Bitkom fügt zwar an, dass „gleichzeitig die Privatsphäre und das Persönlichkeitsrecht der EU-Bürger geschützt werden“ soll, aber es ist nur eine untergeordnete Bedingung und nicht das Ziel der Einflussnahme durch den Bitkom. Dies lässt sich deutlich als Forderung nach wirtschaftsfreundlicheren Regelungen bewerten, die „das Datenschutzrecht nicht überfrachten“ sollen, die europäischen Unternehmen in ihren Möglichkeiten der Datennutzung nicht gegenüber anderen Weltregionen benachteiligen sollen, und generell die „stark verbraucherlastige Sicht“ des Justizministeriums durch eine unternehmensorientierte Sichtweise wieder ins Lot rücken sollen. Hierzu gehöre auch, dass eine nachträgliche Zweckänderung der Datennutzung möglich werden muss, dass die Einwilligungspflichten nicht zu streng gestaltet und eher entschlackt werden, und dass die Pflicht zur Anonymisierung auf ein verhältnismäßiges Maß begrenzt wird. Auf die in der Präambel der EU-Datenschutz-Grundverordnung genannte Notwendigkeit des Schutzes der Bürger*innen geht der Bitkom im ausführlichen Teil der Stellungnahme nicht mehr ein. Auch in weiteren Leitfäden und Handreichungen des Bitkom werden v.a. der wirtschaftliche Nutzen von Big Data hervorgehoben und Hilfen zur Anwendung und Umsetzung von Big-Data-Analysen gegeben (z. B. Bitkom, 2013a; 2015b). An anderer Stelle bemerkt Peter Langkafel, Geschäftsführer der HCB Healthcubator GmbH, auf der Webseite des Bitkom im Hinblick auf die Befürchtung eines gläsernen Patienten durch Big-Data-Anwendungen im Gesundheitswesen, dass ein gläserner Patient nicht das Problem sei, sondern dass „Wir […] die Daten davor schützen [müssen], NICHT benutzt zu werden“ (Langkafel 2016). Hiermit werden Probleme und Gefahren von Big-Data-Anwendungen sehr bewusst delegitimiert, da eine Verweigerung der Datennutzung gleichgesetzt wird mit der Verweigerung zur Rettung von Menschenleben.



"Daten-Dubletten, da sie aus kodierten Kategorien heraus geschaffen werden, sind keine unschuldigen oder harmlosen virtuellen Fiktionen. Während sie im Umlauf sind, eröffnen und schließen sich Zugänge und Möglichkeiten. […] Sie sind ethisch, politisch."

3. Big-Data-Analysen sind nicht neutral
Die Nutzung algorithmischer Entscheidungsfindung auf Basis von Big Data birgt einige Probleme, die besonders relevant sind, wenn sie Entscheidungen über Menschen treffen. Diese spielen in der positiven Bewertung von Big Data für Wissenschaft und Wirtschaft keine zentrale Rolle, werden jedoch in anderen sozialen Welten, z.B. von Bürgerrechtler*innen und einigen Wissenschaftler*innen diskutiert.

Mithilfe großer Datenmengen werden sog. „data doubles“ (Daten-Dubletten) von Menschen geschaffen, die eine Person als eine Summe ihrer Daten abbilden und damit modellieren und in Beziehung zu anderen Daten setzen. Ein einfaches Beispiel: Aufgrund des Wohnortes von Personen werden statistische Aussagen und Verbindungen zu Konsumverhaltensweisen getroffen. Diese sind grundsätzlich nicht neutral, sondern wertend und performativ, d.h. sie haben einen echten Effekt auf das Leben von Menschen. David Lyon z.B. schreibt dazu, dass „Daten-Dubletten, da sie aus kodierten Kategorien heraus geschaffen werden, keine unschuldigen oder harmlosen virtuellen Fiktionen sind. Während sie im Umlauf sind, eröffnen und schließen sich Zugänge und Möglichkeiten. […] Sie bewirken einen echten Unterschied. Sie sind ethisch, politisch.“ (Lyon 2003)

Dies bekommt vor dem Hintergrund einer unterschiedlich stark ausgeprägten Einseitigkeit der algorithmischen Analyse und Entscheidungsfindung eine besondere Bedeutung: Erstens wird als Nachteil der Personalisierung die Konstruktion von Echokammern bzw. „Filterblasen“ (Pariser 2011) genannt, welche ausschließlich schon bestehende Meinungen, Einstellungen oder Informationen widerspiegeln. Zweitens werden computergestützte Entscheidungsfindungsverfahren zwar oft dafür gelobt, weniger empfänglich für menschliche Vorurteile und

Lyon, David (2003): Surveillance as social sorting. Computer codes and mobile bodies. In: David Lyon (Hg.): Surveillance as Social Sorting. Privacy, risk, and digital dis-crimination. London: Routledge, S. 13 – 30.

persönliche Einstellungen zu sein. Dennoch sind gerade maschinenbasierte Entscheidungsprozesse anfällig dafür, „die weitaus massiveren Auswirkungen systemischer Verzerrungen und blinder Flecken im Hinblick auf strukturelle Einschränkungen“ zu normalisieren (Gandy 2010). Bewusste und unbewusste Einseitigkeiten und Werte werden in die Programmcodes und Algorithmen eingeschrieben. Anders gesagt: Algorithmen bekommen Werte und Vorurteile von Programmierer*innen und Auftraggeber*innen vererbt. Diese Algorithmen bestimmen, welche Daten gesammelt, wie sie verknüpft und wie daraus Erkenntnisse gewonnen werden. Solche strukturellen Einseitigkeiten sind kaum nachverfolgbar, weil Algorithmen meist nicht offengelegt werden oder wenn doch, sehr komplex sind und sich mit der Zeit und bei häufiger Nutzung und Erweiterung selbst umschreiben können. Man könnte dem gegenüber stellen, dass alle Technologien in der einen oder anderen Weise Menschen diskriminieren, aber was Diskriminierung durch umfassende Big-Data-Analysen von anderen Technologien unterscheidet, ist das systematische und sowohl „detaillierte [als auch] adaptive Spektrum der Kategorisierungen, die sie produzieren“ können (de Vries 2010). In anderen Worten werden Menschen durch intransparente Prozesse in zahllose Gruppen eingeteilt, die sich ständig wandeln und kaum greifbar sind. Diese Einteilung bildet die Grundlage dafür, dass diese Menschen unterschiedlich behandelt werden.

Darüber hinaus behauptet etwa Guzik, dass „vorhersagendes Data-Mining designbedingt diskriminiert”, weil dessen Kernfunktion darin besteht, bestimmte Personengruppen festzulegen und zu unterscheiden (Guzik 2009). Je nach Bewertung dieser Gruppe hat dies unterschiedlich schwere Auswirkungen. Besonders stark sind diese, wenn Big-Data-Analysen z.B. zur Terrorabwehr oder in anderen Sicherheitsfragen angewandt werden, um verdächtige oder potentiell gefährliche Personen zu finden. In diesem Fall sind deutliche Nachteile bis hin zum Freiheitsentzug für Menschen zu erwarten, die in eine Hochrisiko-Gruppe eingruppiert werden. Alle Mitglieder einer solchen statistisch geschaffenen Gruppe „tragen die Last dieser Überwachungsmethode und der zahllosen Fehler – falsch-positive Meldungen – die sie verursachen wird” (Guzik 2009). Diese falsch-positiven sind genauso wie falsch-negative Meldungen zwangsläufig Bestandteil jeder statistischen Analyse. Wie Guzik weiter ausführt, ist es nicht nur ein Problem, dass diese Personen unschuldig sind und dennoch staatliche Überwachung oder einschränkende Maßnahmen erfahren, die ihre Grundrechte betreffen, sondern es betrifft auch die gerechte Verteilung dieser Kosten/Belastungen in der Gesellschaft ebenso wie die Privatsphäre. Deshalb betreffen solche Gruppeneinteilungen nicht nur individuelle Rechte und Nachteile, sondern sind auch eine Frage der Fairness und sozialen Gerechtigkeit (Guzik 2009). Entscheidungen auf Basis solcher Kategorien und Gruppen zu treffen wird auch „statistische Diskriminierung“ genannt.

Oft wird als Gegenargument angeführt, dass darin kein Problem bestehe, solange diese Diskriminierung einem höheren Ziel diene, wie z.B. einer verbesserten Sicherheit der Gesellschaft (Gandy 2010). Dieser Argumentation folgend wären Entscheidungen zu rechtfertigen, die auch ohne gesicherte Erkenntnisse oder Kausalbeziehungen allein auf Basis von Vermutungen getroffen werden, solange diese zumindest einigermaßen zuverlässig sind.

Eine Bewertung der Zuverlässigkeit ist jedoch kaum möglich, da sich Big-Data-Algorithmen durch eine Analyse ihrer Einordnungen selbst bestätigen können: Wenn z.B. zwei Gruppen unterschieden werden mit dem Zweck, die Personen der zweiten Gruppe stärker auf

verbotene Gegenstände o.Ä. zu untersuchen, so wird diese Untersuchung auch statistisch mehr Treffer in dieser Gruppe zum Vorschein bringen. Damit ist auch nachträglich kaum möglich, durch einen Vergleich der algorithmisch differenzierten Gruppen dieser Differenzierung ihre Untauglichkeit nachzuweisen.

Es bleibt darüber hinaus die grundsätzliche Frage, wie viel Einfluss über Menschen wir bereit sind und sein sollten, Algorithmen zuzugestehen – so gut oder schlecht sie auch arbeiten mögen.

4. Kontextualität und Transparenz

Algorithmen, die Big Data-Analysen zugrunde liegen, werden häufig so programmiert, dass sie bestimmte Korrelationen zwischen Daten erkennen, die dann eine Kategorisierung und Vorhersage ermöglichen, z.B. durch die Einteilung von Menschen in Risikogruppen. Dies benötigt jedoch eine Modellierung der Daten, die sie aus ihrem Kontext herauslöst und in das Datenanalysemodell einpasst. Dabei wird häufig übersehen, dass der Kontext Daten eine spezielle Bedeutung gibt, die aber durch das Herauslösen aus dem Kontext verloren geht (Boyd & Crawford 2012). Diese Dekontextualisierung kann zu Missverständnissen und Fehlinterpretationen führen. Auch wenn Algorithmen darauf ausgelegt sind, Daten zu Mustern zu verknüpfen, ist es keineswegs sicher, dass jede Information auch Teil eines größeren Bildes ist. Boyd und Crawford schreiben in diesem Zusammenhang, dass „Big Data zu häufig die Praxis der Apophänie ermöglicht: Muster zu sehen, wo tatsächlich keine existieren, einfach nur, weil enorme Mengen an Daten Verbindungen zeigen können, die in alle Richtungen ausstrahlen“ (Boyd & Crawford 2012). Auch diese Praxis der Apophänie kann wie alle Formen von Fehlern und Problemen der algorithmischen datenbasierten Entscheidungsfindung für die Betroffenen schwerwiegende Auswirkungen haben. Besonders in Sicherheitsfragen sind diese sehr schwerwiegend und falsche Entscheidungen haben nicht einfach nur unangenehme Folgen, sondern stellen ernstzunehmende Missstände dar. Menschen können aufgrund von ähnlichen Datenmustern falsch eingruppiert, herausgefiltert und bloßgestellt werden, am Reisen gehindert oder unschuldig verhaftet oder gar gefoltert werden (vgl. z.B. die Fälle von Ould Salek oder Maher Arar). Dennoch sind algorithmische Bewertungs- und Entscheidungsroutinen nicht transparent. Sie basieren auf sich ändernden Datenquellen, welche sowohl falsche Daten als auch falsche Analyseroutinen schwer zu entdecken und damit auch schwer in Frage zu stellen machen (Gandy 2010). Der Prozess, der zu Big-Data-basierten Entscheidungen führt, ist praktisch nicht nachvollziehbar und auch für die ausführenden Mitarbeiter*innen oder Beamt*innen praktisch kaum einsehbar. Damit ist es für diese auch kaum möglich, sich über solche Einschätzungen hinwegzusetzen. Hinzu kommt der Glaube an die Technik und die Intelligenz des umfassenden Systems: ‚Bestimmt habe ich etwas übersehen, wenn der Computer zu einem anderen Ergebnis kommt. Er wird schon seine Gründe haben.‘ Induktive algorithmenbasierte Methoden definieren gerade bei Einschätzungen eines verdächtigen Verhaltens aus den Daten heraus eine Norm (des unverdächtigen Verhaltens) und damit auch Muster der Abweichung, die als verdächtig gelten. Ein „algorithmischer Grund“ umgeht damit die bis dato geltenden Evaluierungsmethoden, die nicht nur in der Wissenschaft zur Verbesserung der Robustheit angewendet wurden, wie zum Beispiel Proben, Versuche und Experimente (Rouvroy 2013). „[Datenanalysen, die als] die Überwindung menschlicher Irrationalität bezeichnet worden sind, welche Interpretationen als Quelle von

Fehlern und Diskriminierung umgehen, setzen dann im Grunde genommen die datengetriebene Profilerstellung in eine Black Box“ (Leese 2014). In diese Black Box hineinschauen zu können oder sie zu bewerten, ist entscheidend, wenn es um Menschenrechte geht. Eine der Kernprinzipien westlicher Demokratien besteht darin, dass Bürger*innen das Recht und auch die Möglichkeit haben, staatliche Handlungen kritisch zu hinterfragen und nicht nur abhängig zu sein von staatlicher Macht. Jedoch sind gerade diese Rechte gefährdet, wenn man sich Algorithmen- und Big-Data-basierte Entscheidungsfindung anschaut.

"Es wird schlicht nicht ökonomisch und noch nicht mal technisch umsetzbar sein, dass Datensubjekte die ‘Richtigkeit’ oder Genauigkeit der Daten oder analytischen Modelle, welche [...] genutzt werden, beurteilen und dann anfechten."

Gandy, Oscar H. (2010): Engaging Rational Discrimination: Exploring Reasons for Placing Regulatory Constraints on Decision Support Systems. In: Ethics and Information Technology 12(1), S. 39.

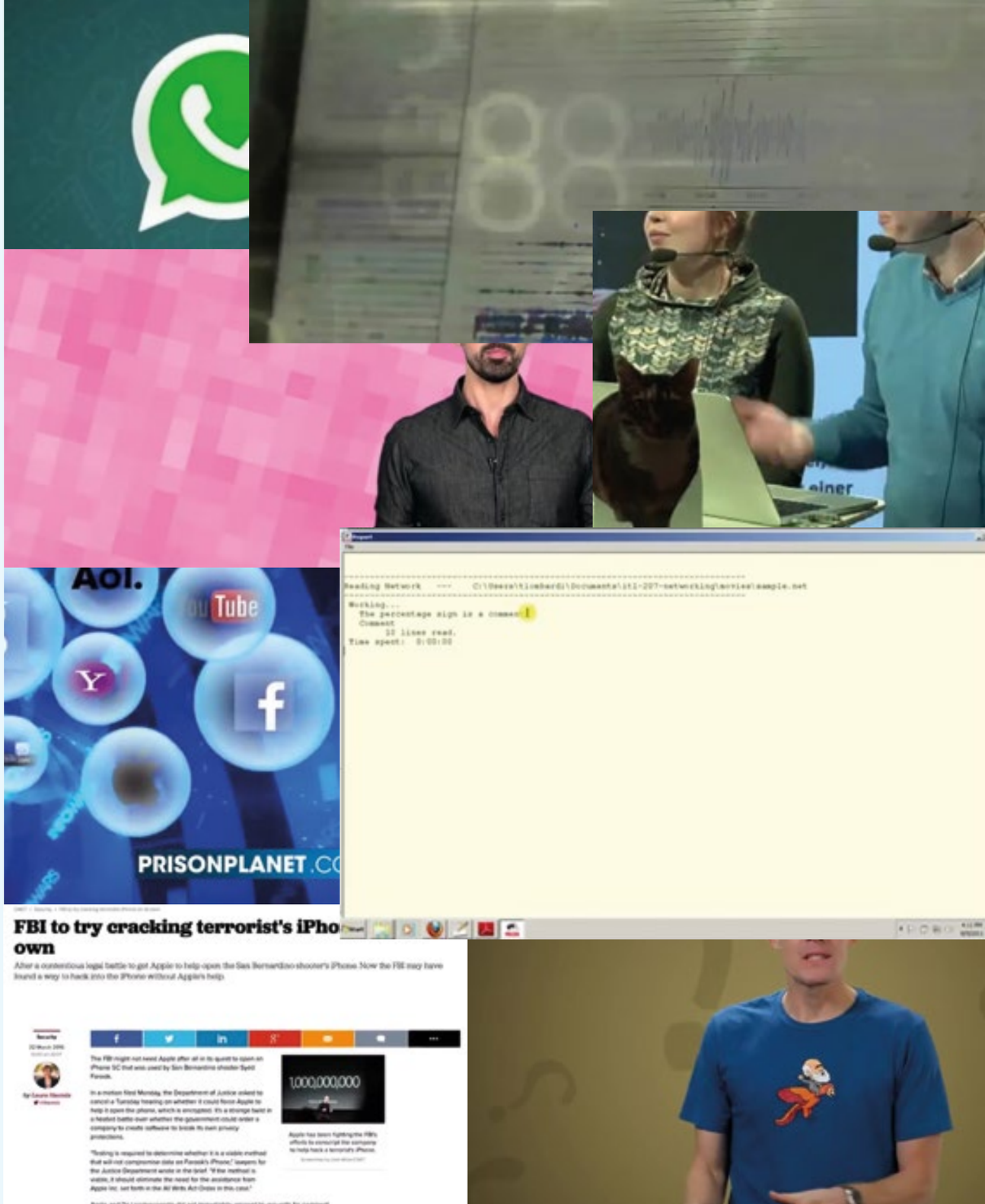
1. „Algorithmische Gouvernementalität vermeidet sorgfältig alle Arten der Konfrontation, insbesondere mit denen, die von ihren Regulierungsauswirkungen betroffen sind" (Rouvroy 2013). Die Menschen können häufig gar nicht wissen, ob und wann sie diskriminiert werden (Gandy 2010).

2. Sollten Menschen dennoch eine Diskriminierung feststellen und gegen sie vorgehen wollen, so ist der Weg der Entscheidung immer noch in der Black Box und es ist nur schwer oder überhaupt nicht möglich, den Fehler auf den Algorithmus oder die Daten zurückzuführen. Selbst wenn man Zugang zum Quellcode des Algorithmus bekommt, ist es sehr schwer, die einzelnen Bestandteile zu unterscheiden und zu analysieren und natürlich ist man angewiesen auf Expert*innen. „Es wird schlicht nicht ökonomisch und noch nicht mal technisch umsetzbar sein, dass Datensubjekte die 'Richtigkeit' oder Genauigkeit der Daten oder analytischen Modelle, welche [...] genutzt werden, beurteilen und dann anfechten" (Gandy 2010). Wenn wir noch selbst-lernende Algorithmen hinzunehmen, ist es praktisch unmöglich.

3. Weiterhin bleibt die Frage der Verantwortlichkeit: Ist es die Schuld des Algorithmus, des/der Programmierer*in oder des/der ausführenden Mitarbeiter*in oder Beamt*in? Oder sind es falsche oder ungenügende Daten?

4. Wenn die Programme und Routinen im Allgemeinen gut funktionieren, unter Aufsicht stehen und bessere Ergebnisse als andere oder frühere Methoden liefern, wird es für die Betroffenen äußerst schwierig zu beweisen, dass sie diskriminiert wurden und dass es nicht ihre eigene Schuld ist, z.B. weil sie zu wenig Daten zur Auswertung bereitgestellt haben und das System daher falsche Schlüsse gezogen hat. Diskriminierte Personen müssen in diesen Fällen gegen eine scheinbar objektive Entscheidung vorgehen.

Dieselben Eigenschaften von Big-Data-Analysen, die für ihre „Objektivität" und Unabhängigkeit von menschlichen (Fehl-)Entscheidungen gelobt werden, erschweren es deutlich, Fragen der Transparenz und Verantwortlichkeit von privaten und staatlichen Akteuren zu stellen und zu beantworten. Besonders wichtig hierbei ist, dass Algorithmen- und datenbasierte Entscheidungsroutinen sowohl bestehende Datenschutz- als auch Nicht-Diskriminierungsgrundsätze, wie sie zum Beispiel in der Europäischen Grundrechtecharta stehen, unterminieren (Guzik 2009).



Ein Algorithmus sucht nach Youtube-Videos zu dem Thema Big Data. Dieser analysiert, klassifiziert und filtert Inhalte. Die daraus extrahierten Videoausschnitte wurden anschließend automatisiert zu einem 16-minütigen Video zusammengeschnitten. Unter folgendem Link finden Sie das Video DATA_DATA_DATA: https://vimeo.com/219681139

LITERATUR

Anderson, Chris (2008): The End of Theory. The Data Deluge Makes the Scientific Method Obsolete. In: Wired.com. http://archive.wired.com/science/discoveries/magazine/16-07/pb_theory [abgerufen am 10.11.2014].

Bitkom (2013): Management von Big-Data-Projekten. https://www.bitkom.org/Bitkom/Publikationen/Management-von-Big-Data-Projekten.html [abgerufen am 25.05.2016].

Bitkom (2015a): Big Data und europäisches Datenschutzrecht. https://www.bitkom.org/LostFound/20150204-Stellungnahme-Big-Data-und-Datenschutz.pdf [abgerufen am 25.05.2016].

Bitkom (2015b): Big Data und Geschäftsmodell – Innovationen in der Praxis: 40+ Beispiele. https://www.bitkom.org/Bitkom/Publikationen/Big-Data-und-Geschaeftsmodell-Innovationen-in-der-Praxis-40-Beispiele.html [abgerufen am 25.05.2016].

Boyd, Danah/Crawford, Kate (2012): Critical questions for Big Data. Provocations for a cultural, technological, and scholarly phenomenon. In: Information, Communication & Society 15(5), S. 662 – 679.

Burkhardt, Marcus (2015): Digitale Datenbanken. Eine Medientheorie im Zeitalter von Big Data. Bielefeld: Transcript.

Cole, David (2014): 'We Kill People Based on Metadata'. In: The New York Review of Books http://www.nybooks.com/daily/2014/05/10/we-kill-people-based-metadata/ [abgerufen am 25.05.2016].

de Vries, Katja (2010): Identity, Profiling Algorithms and a World of Ambient Intelligence. In: Ethics and Information Technology 12(1), S. 71 – 85.

Gandy, Oscar H. (2010): Engaging Rational Discrimination: Exploring Reasons for Placing Regulatory Constraints on Decision Support Systems. In: Ethics and Information Technology 12(1), S. 29 – 42.

Guzik, Kevin (2009): Discrimination by Design: Predictive Data Mining as Security Practice in the United States ‚War on Terror'. In: Surveillance & Society 7(1), S. 3 – 20.

Helbing, Dirk et al. (2015): Digitale Demokratie statt Datendiktatur. In: Spektrum.de. http://www.spektrum.de/news/wie-algorithmen-und-big-data-unsere-zukunft-bestimmen/1375933 [abgerufen am 21.03.2017].

Kitchin, Rob (2014a): Big Data, new epistemologies and paradigm shifts. In: Big Data & Society 1(1), S. 1 – 12.

Kitchin, Rob (2014b): The real-time city? Big data and smart urbanism. In: Geo Journal 79(1), S. 1 – 14.

Langkafel, Peter (2016): Big Data in der Medizin und die Angst vor dem ‚gläsernen Patienten'? https://www.bitkom.org/Presse/Blog/Big-Data-in-der-Medizin-und-die-Angst-vor-dem-glaesernen-Patienten.html [abgerufen am 25.05.2016].

Leese, Matthias (2014): The New Profiling: Algorithms, Black Boxes, and the Failure of Anti-discriminatory Safeguards in the European Union. In: Security Dialogue 45(5), S. 494 – 511.

Lyon, David (2003): Surveillance as social sorting. Computer codes and mobile bodies. In: David Lyon (Hg.): Surveillance as Social Sorting. Privacy, risk, and digital discrimination. London: Routledge, S. 13 – 30.

Manovich, Lev (2014): Trending. Verheißungen und Herausforderungen der Big Social Data. In: Ramón Reichert (Hg.): Big Data. Analysen zum digitalen Wandel von Wissen, Macht und Ökonomie. Bielefeld: Transcript, S. 65 – 83.

Mayer-Schönberger, Viktor / Cukier, Kenneth (2013): Big Data. A Revolution That Will Transform How We Live, Work, and Think. New York: Eamon Dolan.

Nissenbaum, Helen (2010): Privacy in Context. Technology, Policy, and the Integrity of Social Life. Stanford: Stanford University Press.

Pariser, Eli (2011): The Filter Bubble. What the Internet Is Hiding from You. New York: The Penguin Press.

Reichert, Ramón (Hg.) (2014): Big Data. Analysen zum digitalen Wandel von Wissen, Macht und Ökonomie. Bielefeld: Transcript.

Rouvroy, Antoinette (2013): The End(s) of Critique: Data-behaviourism vs. Due-process. In: Hildebrandt, Mireille/de Vries, Katja (Hg.): Privacy, Due Process and the Computational Turn. The Philosophy of Law Meets the Philosophy of Technology. Milton Park/New York: Routledge, S. 143 – 68.

Vayena, Effy/Salathé, Marcel/Madoff, Lawrence C./Brownstein, John S. (2015): Ethical challenges of big data in public health. In: PLoS Comput Biol 11 (2), S. 1 – 7.

Vedder, Anton (1999): KDD: The challenge to individualism. In: Ethics and Information Technology 1(4), S. 275 – 281.

Welzer, Harald (2016): Die smarte Diktatur. Der Angriff auf unsere Freiheit. Frankfurt a.M: Fischer Verlag.

NATIONS'
DATA"

Center for American Progress
www.americanprogressac

cal clustering

ive clustering:
each vertex to a group of its own
wo groups with the highest similarity and join them in a single

te similarity between groups:
-linkage clustering (most similar in the group)
lete-linkage clustering (least similar in the group)
ge-linkage clustering (mean similarity between groups)
until all joined into single group

Dendrogram

nate advances bill ending govt.

w.presstv.ir facebook.com/presstv

arkar | Modern Big Data An

Great Wide G

S COURT BACKS NSA, JUDGE
TS ENDING MASS SURVEILLANCE

User-based collaborative filtering

- Collaborative filtering is the most prominent approach to generate recommendations
  - **User-based:** find similar users to current user and look at their likes and dislikes to predict interests of current user
  - **Item-based:** use same data (user rankings) but find items near current item
  - **Content-based:** use different data – find items with similar properties
- Basic assumption and idea is that users give ratings to "items"
  - Customers who had similar tastes in the past, will have similar tastes in the future
- Input is a matrix of user–item ratings
- Output is a (numerical) prediction indicating to what degree the current user will like or dislike **each item**
- Look at all items in this way and **return top-ranked items for this user**
- Difficult as need to evaluate all item ratings for each user; in alternative item-based, one can find out INDEPENDENTLY of user, which items are near a given item

Datenschutz-Grundverordnung

von Charlotte Barlag, Barbara Büttner, Christian Geminn, Nadine Miedzianowski

DIE AUSEIN-ANDERSET-ZUNGEN UM DIE ZUKUNFT DES EUROPÄISCHEN DATENSCHUTZES

06

1 Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates v. 27.04.2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG, ABl. 119/1 (im Folgenden als „Datenschutz-Grundverordnung" oder „Verordnung" bezeichnet).

2 Europäische Kommission 2012.

3 Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr v. 25.1.2012, KOM (2012) 11 endg., 2012/0011 (COD).

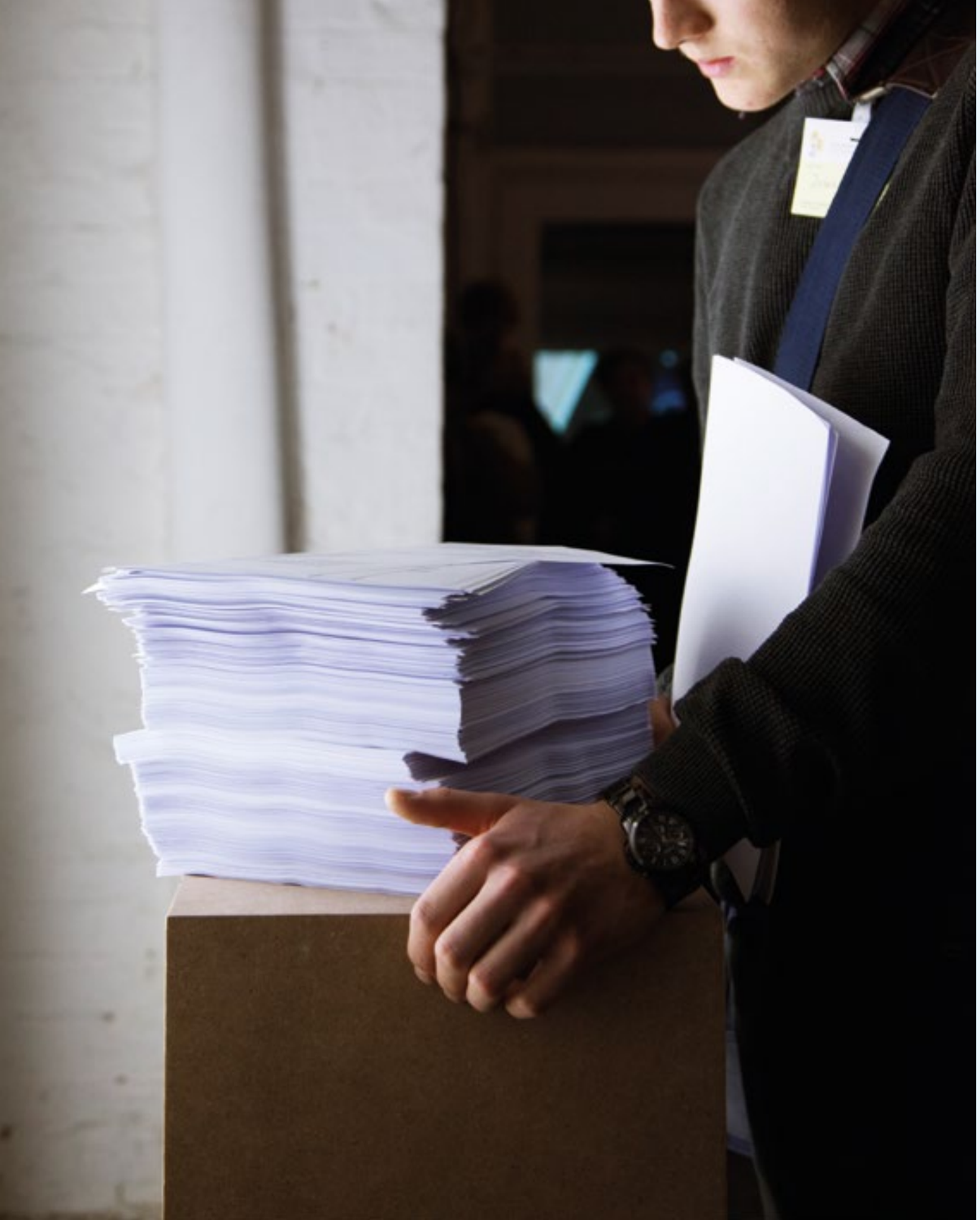
1. Neue Unsicherheiten aufgrund der digitalen Verarbeitungsmöglichkeiten personenbezogener Daten

Von Januar 2012 bis Dezember 2015 wurde in Brüssel die europäische Datenschutz-Grundverordnung[1] verhandelt. Sie wird ab Ende Mai 2018 in der gesamten Europäischen Union geltendes Recht sein. Die Verordnung bringt eine fundamentale Überarbeitung und Neuordnung des Datenschutzrechts in Europa mit sich.

Mit diesen Worten begann Viviane Reding, seinerzeit EU-Kommissarin für Justiz, Grundrechte und Bürgerschaft sowie Kommissionsvizepräsidentin, die Vorstellung des Kommissionsentwurfs der Datenschutz-Grundverordnung am 25.1.2012.[3]

„Vor 17 Jahren nutzten weniger als 1% der Bevölkerung das Internet. Heute werden große Mengen an personenbezogenen Daten übermittelt und ausgetauscht, über den gesamten Globus – innerhalb von Bruchteilen von Sekunden."[2]

Die Vernetzung nahezu aller Lebensbereiche ist in den vergangenen Jahren massiv fortgeschritten. „Smart Home", „Smart Car" und „Smart City" stehen exemplarisch für das Ubiquitous Computing – die allgegenwärtige rechnergestützte Informationsverarbeitung. So werden derzeit immer mehr Gegenstände miteinander vernetzt, weshalb sich auch der Begriff „Internet der Dinge" durchgesetzt hat. Durch die Digitalisierung entstehen enorme Datenmengen, die etwa Big Data-Anwendungen möglich machen und die Voraussetzung für umfangreiche Profilbildungen darstellen. Zudem steigt die Zahl datengetriebener Geschäftsmodelle, denn mit den gesammelten Daten lässt sich etwa gezielt werben, sodass diesen Daten ein nicht unerheblicher Vermögenswert zukommt. Daneben eröffnen sich auch für Geheimdienste bisher ungeahnte Möglichkeiten der Informationskontrolle. Dem Nutzen und Komfort smarter Anwendungen stehen daher die Möglichkeit der Verletzung von Persönlichkeitsrechten und die Verunsicherung althergebrachter Routinen der Privatheit gegenüber. Privatheit wird in dieser Situation zu einem zentralen Streitgegenstand. Dabei ist jedoch



selten klar, was Privatheit überhaupt sein soll – etwa ein zentraler Grundstein für eine gelingende Demokratie oder doch ein längst überholtes Konzept – noch wie in Zukunft damit umgegangen werden soll. Im Angesicht der grundlegenden Irritation der Privatheitsroutinen und -praktiken versammeln sich verschiedene Akteure und Instanzen um den Gegenstand der Privatheit und versuchen Lösungen für diese neuen Unsicherheiten der Digitalisierung zu finden. Dabei prallen nicht nur verschiedene Ansätze mit dem Problem umzugehen, sondern auch unterschiedliche Interessen und Problemdeutungen aufeinander. Der Vorschlag zur Datenschutz-Grundverordnung war einer dieser Lösungsansätze, der versuchte den neuen Herausforderungen mit Hilfe einer rechtlichen Regelung auf europäischer Ebene zu begegnen. Der Ansatz der Einführung einer Verordnung kann somit als eine Reaktion auf die Krise der Privatheit verstanden werden, ausgelöst durch die Unsicherheiten in Zeiten digitaler Transformationen und deren Implikationen für Privatheit. Privatheit wird in diesen Reaktionen selten isoliert verhandelt, vielmehr geht es immer auch um die Gestaltung der digitalen Welt insgesamt.

Die Europäische Kommission[4] hat den Reformprozess der EU-Datenschutzvorschriften aus dem Jahr 1995 im Januar 2012 angestoßen.[5] Die Datenschutzrichtlinie[6] litt nach Auffassung der Kommission vor allem an zwei Schwachstellen, die es zu beheben galt: Sie entstand in einer Zeit, in der das Internet noch in den Kinderschuhen steckte und war daher für eine Art der Datenerfassung und Datenverarbeitung konzipiert, die sich zwischenzeitlich grundlegend verändert hatte. Zudem fehlte es an einem einheitlichen europäischen Datenschutzrecht. Die 27 EU-Mitgliedstaaten hatten die Vorschriften der Richtlinie unterschiedlich umgesetzt, was zu teils großen Unterschieden im Datenschutzniveau einzelner Mitgliedstaaten führte[7] und mit Kosten für die Wirtschaft und mit Rechtsunsicherheit auf Seiten der Bürger*innen verbunden war. Um diese Probleme zu beheben, trat die Datenschutz-Grundverordnung mit den Zielen einer umfassenden Modernisierung und Harmonisierung des Datenschutzes in Europa an, um zum einen die Rechte der EU-Bürger*innen zu schützen und die Umsetzung der Grundrechte auf Schutz des Privatlebens aus Art.7 und auf Schutz personenbezogener Daten aus Art. 8 GRCh zu gewährleisten. Zum anderen wollte die Kommission gleichzeitig das Wirtschaftswachstum ankurbeln und damit die Wettbewerbsfähigkeit der Europäischen Union steigern. Dies sollte auf zwei verschiedenen Wegen erreicht werden. Einerseits mittelbar

4 Im Folgenden auch „Kommission“ genannt.

5 Mitteilung der Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen, „Der Schutz der Privatsphäre in einer vernetzten Welt – Ein europäischer Datenschutzrahmen für das 21. Jahrhundert“, v. 25.1.2012, KOM (2012) 9 endg., 5.

6 Richtlinie 95/46/EG des Europäischen Parlaments und des Rates v. 24.10.1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr, ABl. L 281/31; im Folgenden auch „Richtlinie“ genannt.

7 Europäischen Kommission 2012.

über den Grundrechtsschutz. Ein hohes Datenschutzniveau soll das Vertrauen der europäischen Verbraucher*innen in Online-Dienste stärken und so die digitale Wirtschaft ankurbeln. Andererseits soll ein einheitlicher Rechtsrahmen auf EU-Ebene Hindernisse für den Marktzutritt überwinden und so weiteres Wirtschaftswachstum generieren.

Macht man sich die unterschiedlichen Ziele deutlich, so wird schnell verständlich, warum es sich um einen schwierigen und langwierigen Reformprozess gehandelt hat. Der Schutz personenbezogener Daten, wie er in Art. 8 Abs. 1 GRCh verankert ist, ist kein Selbstzweck, sondern dient dem Schutz der informationellen Selbstbestimmung des Einzelnen. Gleichzeitig kann er aber auch Mittel zur Durchsetzung wirtschaftlicher Interessen sein, obwohl er teilweise in eklatantem Widerspruch zu diesen wirtschaftlichen Interessen steht.

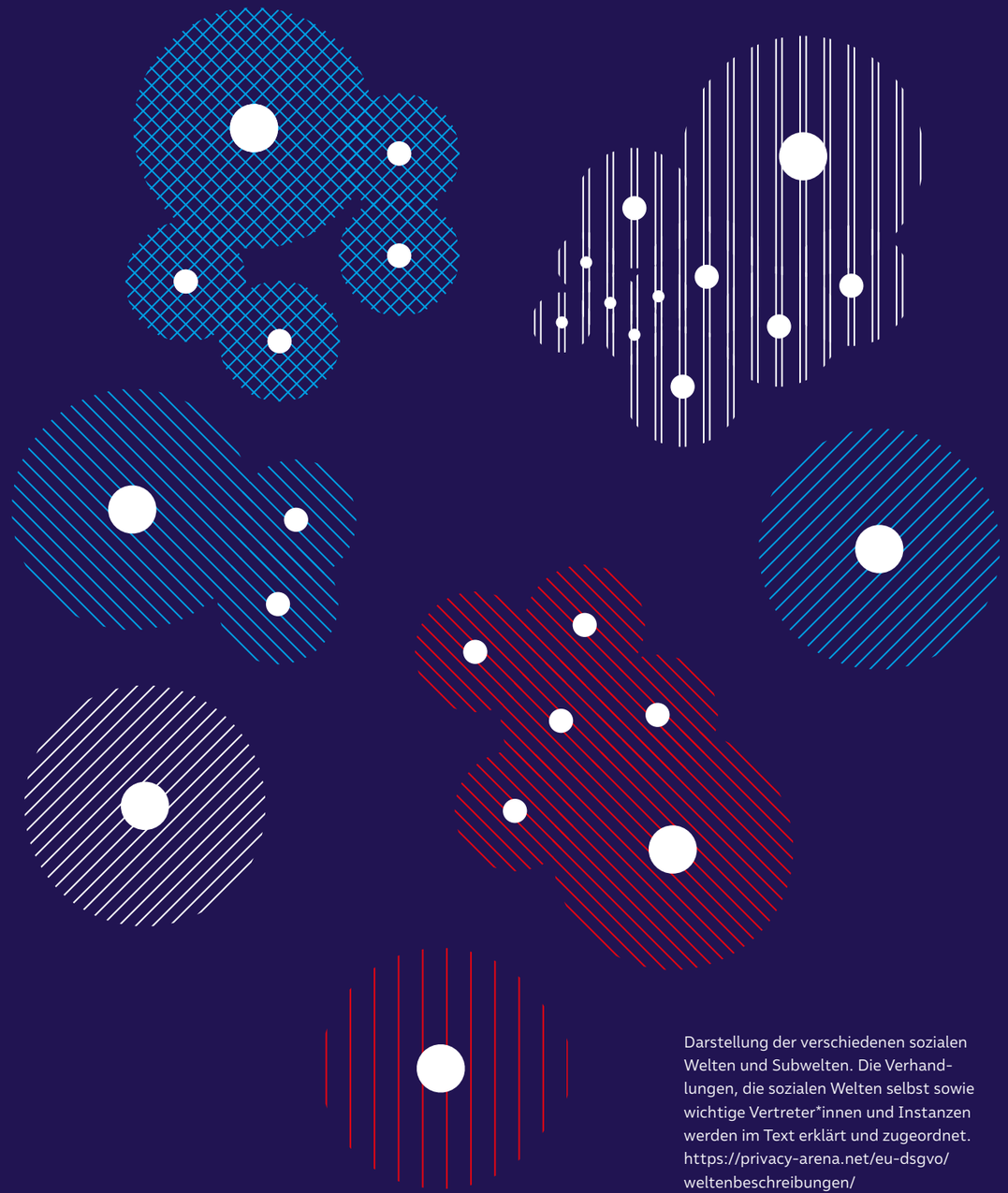
Vorgehensweise

Die nachfolgenden Analysen der Datenschutz-Grundverordnung konzentrieren sich auf die Verhandlungen nach Bekanntgabe des Kommissionsentwurfs am 25. Januar 2012, wodurch das Gesetzgebungsverfahren offiziell eröffnet wurde. Die Verhandlungen rund um die Verordnung dauerten insgesamt vier Jahre. Während dieser Zeit versammelten sich verschiedene Akteure und Instanzen um den Streitgegenstand der „Datenschutz-Grundverordnung" und diskutierten und kämpften um ihre Ausgestaltung. Dabei ging es selten nur um den Streitgegenstand selbst. Vielmehr wurden verschiedene Interessen und Deutungen mitverhandelt, die die digitale Welt insgesamt betreffen; sei es nun der Stellenwert ökonomischer Interessen in modernen Nationalstaaten oder ein bestimmtes Verständnis davon, wie demokratische Gesellschaften gestaltet und regiert werden sollten. In den Verhandlungen trafen all diese verschiedenen Interessen, Ziele und Werte aufeinander. Diese sind nicht zwangsläufig an einzelne Akteure gebunden.[8] Deshalb konzentriert sich die Analyse auf verschiedene soziale Welten und deren Vertreter*innen.[9] Soziale Welten können als kollektive Akteure verstanden werden, denen eine geteilte Kernpraktik gemein ist, d.h. eine Aktivität, die alle Mitglieder der sozialen Welt ausüben (Bsp. Verwertung personenbezogener Daten zur Profitgenerierung). Diese Tätigkeit wird meist auf eine bestimmte Art und Weise ausgeführt, man könnte auch sagen sie folgt im weitesten Sinne einer bestimmten Technik (Bsp. Schreiben von Algorithmen). Schließlich finden die Tätigkeiten an einem bestimmten Ort statt (Bsp. Bürogebäude). Vertreten werden die sozialen Welten i.d.R. durch verschiedene Repräsentant*innen, beispielsweise Wirtschaftslobbyist*innen als Vertreter*innen der Welt der Digitalwirtschaft. Soziale Welten sind nicht als statische Gebilde zu verstehen; ihre Grenzen und Ordnungen sind fluide. Welten können mit anderen Welten in Beziehung treten, sich austauschen, Verhandlungen eingehen, Kompromisse schließen bis hin zum Führen von harten Auseinandersetzungen und Kämpfen. Eine Welt kann in sich widersprüchlich sein und aus Uneinigkeiten können neue Subwelten hervorgehen. Auch nicht-menschliche Komponenten wie das Recht selbst beeinflussen den Verhandlungsprozess.[10] Im Folgenden wird aufgezeigt, welche Welten und wichtigen Vertreter*innen an den Aushandlungen um die Datenschutz-Grundverordnung beteiligt waren, welche Positionen sie eingenommen haben und wie sich die Verhandlungen im Zeitverlauf entwickelten.

8 Jemand kann als Mitglied eines Unternehmens großes Interesse an der Verwertung von Daten haben und sich als Elternteil gleichzeitig für den Datenschutz der eigenen Kinder einsetzen.

9 Strauss 1978; Strauss 1993; Clarke 2005.

10 Beispielsweise stecken rechtliche Normen den Handlungsspielraum zahlreicher Akteure zu einem gewissen Grad ab und wirken so mittelbar auf den Verhandlungsprozess ein.



Darstellung der verschiedenen sozialen Welten und Subwelten. Die Verhandlungen, die sozialen Welten selbst sowie wichtige Vertreter*innen und Instanzen werden im Text erklärt und zugeordnet. https://privacy-arena.net/eu-dsgvo/weltenbeschreibungen/

11 Europäische Union o. J. a.

12 Europäische Union o. J. b.

2. Die Arena der Datenschutz-Grundverordnung als Versammlung verschiedener Welten

Um zu verstehen, wer in dieser „Arena der Datenschutz-Grundverordnung" warum welche Interessen vertrat, folgt eine Beschreibung der an den Verhandlungen beteiligten sozialen Welten und der im Verhandlungsprozess relevanten kollektiven Akteure und Instanzen.

2.1 Die Welt der Europäischen Union

Die Datenschutz-Grundverordnung setzt als rechtlicher Lösungsansatz auf europäischer Ebene an. Die europäische Union spielt somit in den Verhandlungen der Datenschutz-Grundverordnung eine rahmengebende Rolle, insofern sie zumindest formal die institutionellen Infrastrukturen und Leitlinien des Gesetzgebungsprozesses mitbestimmt. Anfänglich mit dem Ziel der Förderung der wirtschaftlichen Zusammenarbeit gegründet, deckt die Europäische Union heute zahlreiche Politikfelder ab.[11] Sie hat die Möglichkeit in bestimmten Bereichen eigenständig Recht zu setzen. Die Mitgliedstaaten behalten aber ihre Souveränität und haben nur einzelne Souveränitätsrechte zugunsten einer Überstaatlichkeit an die Europäische Union übertragen. Dies hat dazu geführt, dass das Unionsrecht die Rechtsordnungen der Mitgliedstaaten überlagern und ersetzen kann, um zugunsten des Integrationsprozesses eine eigenständige, staatenübergreifende Rechtsordnung zu gewährleisten. Die Welt der Europäischen Union versucht beständig die eigene Stellung als politischer Akteur auszubauen, ihre Handlungsfähigkeit zu stärken und die Integration der Europäischen Union voranzutreiben.[12]

Der Integrationsprozess verläuft jedoch bis heute auf unterschiedlichen Ebenen (wirtschaftlich, rechtlich, sozial, etc.) und in unterschiedlichen Geschwindigkeiten. Dabei ringt die Welt der Europäische Union immer wieder mit ihrer eigenen Identität und ihrem Selbstverständnis wahlweise als Wirtschaftsunion, Rechtsunion oder Werteunion. Gerade diese unterschiedlichen Vorstellungen davon, wie die Integration gelingen kann, führen innerhalb der Welt zu Konflikten. So herrschte während der Verhandlungen immer wieder Uneinigkeit darüber, ob die Datenschutz-Grundverordnung vordringlich dem Schutz der Grundrechte oder der Stärkung des europäischen Binnenmarkts dienen soll.

13 Die Wahl der Form und Mittel ist jedoch den staatlichen Stellen überlassen. Richtlinien richten sich damit nicht direkt an die Bürger*innen, sondern an die Mitgliedstaaten, die verpflichtet sind, die Richtlinie binnen einer festgelegten Frist in nationales Recht umzusetzen.

14 Der deutsche Bundesrat erhob sogar eine Subsidiaritätsrüge gegen den Entwurf der Kommission; vgl. auch beispielhaft Roßnagel/Kroschwald 2014: S. 495.

15 Vgl. hierzu ausführlich Roßnagel 2017.

Recht der Europäischen Union

Das Unionsrecht kann keiner der herkömmlichen Rechtskategorien zugeordnet werden. Es handelt sich weder um nationales noch um internationales Recht oder um Völkerrecht. Aus diesem Grund wird das Unionsrecht auch als supranationales Recht bezeichnet. Es regelt Rechtsbeziehungen zwischen den EU-Organen untereinander, zwischen der Europäischen Union und den einzelnen Mitgliedstaaten, zwischen den Mitgliedstaaten untereinander, zwischen der Europäischen Union und natürlichen Personen sowie Unternehmen der Mitgliedstaaten sowie zwischen den Mitgliedstaaten und natürlichen Personen und auch zwischen der Union und Drittstaaten.

Soweit ein Rechtsakt der Europäischen Union unmittelbare Wirkung entfaltet, richtet er sich zum einen direkt an die Unionsbürger*innen, sodass diesen daraus Rechte und Pflichten entstehen können. Zum anderen müssen die Gerichte und die Verwaltung diesen Rechtsakt wie das nationale Recht anwenden. Das Unionsrecht genießt gegenüber dem nationalen Recht grundsätzlich einen Anwendungsvorrang, sodass entgegenstehendes nationales Recht unanwendbar wird.

Eine Verordnung hat allgemeine Geltung, ist in allen ihren Teilen verbindlich und gilt unmittelbar in jedem Mitgliedstaat. Verordnungen entsprechen damit auf nationaler Ebene einem Gesetz. Die Datenschutz-Grundverordnung ist eine solche Verordnung und genießt somit Anwendungsvorrang vor dem nationalen Datenschutzrecht. Im Gegensatz dazu ist eine Richtlinie für jeden Mitgliedstaat nur hinsichtlich ihres zu erreichenden Ziels verbindlich.[13] Das bedeutet, dass der Inhalt der Richtlinie von den Mitgliedstaaten in nationales Recht umzusetzen ist. Großbritannien, Dänemark, Slowenien und Ungarn haben sich daher im Laufe der Verhandlungen zur Grundverordnung dafür ausgesprochen, statt der Verordnung eine neue Datenschutzrichtlinie zu erlassen. Auch in Deutschland wurde dieser Wunsch geäußert.[14]

Die nationalen Datenschutzgesetze verlieren mit Inkrafttreten der Verordnung aber nicht ihre Wirksamkeit, sie dürfen nur dann nicht angewendet werden, wenn sie dem Unionsrecht entgegenstehen.[15] Dennoch drängte insbesondere der Rat der Europäischen Union darauf den öffentlichen Bereich mit Hilfe von Öffnungsklauseln aus der Verordnung auszunehmen.

16 Europäische Kommission 2012.

17 Europäische Kommission, Vorschlag für Verordnung des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr ("Datenschutz-Grundverordnung") v. 25.01.2012, 2012/0011 COD, http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_de.pdf.

Europäische Kommission

„Der Schutz personenbezogener Daten ist zwar ein Grundrecht aller Europäer, aber die EU-Bürger haben nicht immer das Gefühl, dass sie vollständige Kontrolle über ihre personenbezogenen Daten haben. Die heute vorgeschlagenen Änderungen werden das Vertrauen in Onlinedienste stärken, weil die Bürger künftig besser über ihre Rechte informiert sein und größere Kontrolle über ihre Daten haben werden. Die Reform wird zudem die Geschäftstätigkeit der Unternehmen einfacher und kostengünstiger machen. Eine straffe, eindeutige und einheitliche Regelung auf EU-Ebene wird dazu beitragen, das Potenzial des digitalen Binnenmarkts freizusetzen und Wirtschaftswachstum, Innovation und Beschäftigung zu fördern.“[16]

(Viviane Reding, damalige Vorsitzende der Europäischen Kommission)

Die Europäische Kommission gab den entscheidenden Impuls für die Reform des europäischen Datenschutzrechts und präsentierte im Januar 2012 den Gesetzesentwurf für eine Datenschutz-Grundverordnung.[17] Die meisten europäischen Rechtsakte können nur auf Initiative der Kommission erlassen werden. Der Entwurf zielte auf ein einheitliches und modernisiertes Datenschutzrecht mit praxisgerechten und rechtsklaren Vorgaben innerhalb der Europäischen Union ab. Dabei sollte für die neuen Datenverarbeitungspraktiken und datengetriebenen Geschäftsmodelle ein einheitlicher rechtlicher Rahmen geschaffen werden. Zugleich sollten aber auch die Rechte der EU-Bürger*innen geschützt werden. Beispielhaft

18 Europäisches Parlament 2014.

19 Im Folgenden auch „Parlament“ genannt.

20 Jan Philipp Albrecht ist Abgeordneter des Europäischen Parlaments für „Die Grünen/EFA“ und für die Datenschutz-Grundverordnung zuständiger Berichterstatter des Parlaments.

hierfür sind das „Recht auf Vergessenwerden“, die Grundsätze „Privacy-by-Design“ und „Privacy-by-Default“ sowie die Wahrung des Verhältnismäßigkeitsprinzips.

Europäisches Parlament

„Ich habe eine klare Botschaft für den Rat: Jede weitere Verschiebung wäre unverantwortlich. Die Bürger Europas erwarten von uns, dass wir eine starke EU-weite Datenschutzverordnung verabschieden. Wenn einige Mitgliedstaaten nach zweijährigen Verhandlungen nicht liefern wollen, dann sollte die Mehrheit ohne sie voranschreiten.“[18]

(Jan Philipp Albrecht, Abgeordneter des Europäischen Parlaments)

Das Europäische Parlament[19] ist das einzige Organ, das direkt von den Unionsbürger*innen gewählt wird. Innerhalb des Parlaments sind verschiedene Parteien und Gruppierungen vertreten, es gibt aber anders als in den nationalen Parlamenten keine Regierungs- und Oppositionsfraktionen. Die Abgeordneten unterliegen damit keinem Koalitionszwang und können flexibler auf Gesetzesentwürfe reagieren. Gleichwohl sind die Parlamentarier in Fraktionen organisiert.

Das Parlament nahm seine Arbeit nach der Veröffentlichung des Kommissionsentwurfs zur Datenschutz-Grundverordnung am 25. Januar 2012 auf. Nachdem der Rechtsausschuss des Europäischen Parlaments dem Ausschuss für bürgerliche Freiheiten, Justiz und Inneres (LIBE) im Oktober 2012 eine Stellungnahme zum Vorschlag für eine Datenschutz-Grundverordnung zukommen ließ, stellte Jan Philipp Albrecht[20] am 9. und 10. Januar 2013 einen etwa 200 Seiten umfassenden Berichtsentwurf mit Änderungen zur Datenschutz-Grundverordnung vor. Nach langem Ringen um

21 Standpunkt des Europäischen Parlaments festgelegt in erster Lesung am 12. März 2014 im Hinblick auf den Erlass der Verordnung (EU) Nr. .../2014 des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Datenschutz-Grundverordnung) (EP-PE_TC1-COD(2012)0011) v. 12.03.2014, http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+TC+P7-TC1-COD-2012-0011+0+DOC+PDF+V0//DE.

22 Rat der Europäischen Union 2015.

den Parlamentsvorschlag und der Bearbeitung von über 3.000 Änderungsanträgen, verabschiedete das Europäische Parlament ihn mit einer Mehrheit von über 95 Prozent der abgegebenen Stimmen. Der Vorschlag wurde sodann im Rat weiter verhandelt. Der Entwurf des Parlaments forderte unter anderem eine frei abgegebene und spezifische Einwilligung des Betroffenen und sah Höchststrafen für Datenschutzverstöße von bis zu 100 Millionen Euro oder fünf Prozent des Jahresumsatzes eines Unternehmens vor,[21] wohingegen die EU-Kommission noch von maximal zwei Prozent des Geschäftsvolumens sprach. Ebenso befürwortete das Parlament das Recht auf Vergessenwerden sowie die Möglichkeit der Datenportabilität. Die Anforderungen für das Erstellen von Persönlichkeitsprofilen wurden verschärft. Für die Übermittlung von Daten europäischer Bürger*innen an Drittstaaten sollte jede Firma eine vorherige Genehmigung einer nationalen Datenschutzbehörde benötigen.

Rat der Europäischen Union

„Heute sind wir einem modernen und einheitlichen Rahmen für den Datenschutz in der Europäischen Union einen großen Schritt näher gekommen. Ich bin sehr zufrieden, dass wir nach über drei Jahren Verhandlungen endlich einen Kompromiss über den Text erzielt haben. Mit der neuen, an die Erfordernisse des digitalen Zeitalters angepassten Datenschutzverordnung werden die individuellen Rechte unserer Bürger gestärkt und ein hohes Schutzniveau gewährleistet.“[22]

(Dzintars Rasnačs, Lettischer Justizminister)

23 Im Folgenden auch „Rat“ genannt.

24 Rat der Europäischen Union, Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Datenschutz-Grundverordnung) v. 11.06.2015, 2012/0011 COD, http://data.consilium.europa.eu/doc/document/ST-9565-2015-INIT/de/pdf.

Der Rat der Europäischen Union[23] besteht aus je einem/r Vertreter*in jedes Mitgliedstaats auf Ministerebene. Er hat im Gegensatz zu den anderen europäischen Institutionen keine ständigen Mitglieder, vielmehr tagt er in unterschiedlichen Zusammensetzungen, je nach betreffender Angelegenheit. Im Gegensatz zum Parlament sind Verhandlungen des Rats nicht öffentlich zugänglich. Die Datenschutz-Grundverordnung ist unter dem luxemburgischen und dem niederländischen Ratsvorsitz entstanden.

Der Rat ist das Bindeglied zwischen der Europäischen Union und den Mitgliedstaaten. Während idealtypisch gesprochen die Europäische Kommission und das Europäische Parlament europäische Interessen verfolgen, vertreten die Ratsmitglieder die Interessen der Mitgliedstaaten, die sie entsenden. Insgesamt gestaltete sich der Verhandlungsprozess des Rats aufgrund interner Streitigkeiten und auseinanderklaffender Interessenlagen der einzelnen Länder sehr zäh. Am 6. Juni 2013 scheiterte der Entwurf einer Datenschutzverordnung der irischen Ratspräsidentschaft im Rat der Europäischen Union. Nach langen Verzögerungen einigte sich der EU-Ministerrat am 15. Juni 2015 schließlich auf eine gemeinsame Fassung der Verordnung.[24]

Der Europäische Gerichtshof
Der Europäische Gerichtshof (EuGH) hat die Aufgabe das Unionsrecht bei dessen Auslegung und Anwendung zu bewahren. Er soll für die einheitliche Interpretation des EU-Rechts und die Achtung des Rechts durch die EU-Staaten und Institutionen sorgen. Der Europäische Gerichtshof bildet zusammen mit dem Gericht der Europäischen Union (EuG) und dem Gericht für den öffentlichen Dienst (EuGöD) den Gerichtshof der Europäischen Union.
Der Europäische Gerichtshof wird mit Inkrafttreten der Datenschutz-Grundverordnung einen deutlichen Zuwachs an Einfluss im Bereich des Datenschutzrechts gewinnen. Viele Fragen der praktischen Ausgestaltung der neuen Verordnung sind noch nicht geregelt und werden zum Teil vor Gericht geklärt werden müssen.

25 Merkel 2015.

2.2 Die Welt der Nationalstaaten

Die Welt der Nationalstaaten vertritt und verteidigt ihre nationalstaatlichen Interessen. Die Praktiken des Regierens sind dabei stets an nationalstaatliche Territorien gebunden. Die Datenschutzinteressen der einzelnen Mitgliedsländer variieren entsprechend je nach den verschiedenen Datenschutzkulturen sowie den wirtschaftlichen und politischen Bedingungen, die vor Ort herrschen. Diese Diversität erschwert die Kompromissbildung zwischen den Nationalstaaten und führte in den Verhandlungen um die Datenschutz-Grundverordnung immer wieder zu Verzögerungen. Während der Verhandlungen haben insbesondere Großbritannien sowie die Bundesrepublik Deutschland den Einigungsprozess gebremst. Die USA wiederum verfolgten in den Debatten eigene Interessen und versuchten den Verhandlungsprozess zu ihren Gunsten zu beeinflussen. Ebenfalls immer wieder Gegenstand der Diskussionen war Irland, das als europäischer Zufluchtsort vieler Firmen galt, die strenge Datenschutzregeln umgehen wollten.

Bundesrepublik Deutschland
Als wirtschaftlich leistungsfähigster und bevölkerungsreichster Mitgliedstaat der Europäischen Union hat die Bundesrepublik Deutschland großes Gewicht bei Entscheidungen auf europäischer Ebene – auch beim Datenschutz.

„Wir müssen hohe Datensicherheit haben, aber wenn wir uns das Big Data Management, wenn wir uns die Möglichkeit der Verarbeitung großer Datenmengen durch einen falschen rechtlichen Rahmen zu sehr einengen, dann wird nicht mehr viel Wertschöpfung in Europa stattfinden. Das wäre für uns von großem Nachteil.“[25]
(Angela Merkel)

26 Im Zuge der Snowden-Veröffentlichungen im Sommer 2013 schien sich diese Position kurzzeitig zu einer datenschutzfreundlicheren Position hin aufzuweichen. Dies zeigte sich auch im Koalitionsvertrag aus dem Jahr 2013. Jedoch war dieser Effekt nur von kurzer Dauer.

27 Antrag der Abgeordneten Dr. Konstantin von Notz, Luise Amtsberg, Volker Beck (Köln), Katja Keul, Renate Künast, Monika Lazar, Irene Mihalic, Özcan Mutlu, Hans-Christian Ströbele und der Fraktion BÜNDNIS 90/DIE GRÜNEN zu dem Vorschlag einer EU-Datenschutzverordnung KOM (2012) 11, Stellungnahme gegenüber der Bundesregierung, 10.06.2015, BT-Drs. 18/5102 S. 2.

28 Klein 2014.

Bundesregierung

Die Bundesregierung ist mit ihren Minister*innen im Rat der Europäischen Union vertreten. In den Verhandlungen zur Datenschutz-Grundverordnung galt die Bundesregierung fast durchgängig als Vertreterin einer eher wirtschaftsfreundlichen Position.[26]

Bundestag

„Der Deutsche Bundestag fordert die Bundesregierung darüber hinaus auf, sich von Anbeginn der bereits für Juni 2015 angesetzten Trilogverhandlungen für weitere Verbesserungen einzusetzen, mit denen ein höchstmögliches Schutzniveau für die Bürgerinnen und Bürger erzielt und keinesfalls weiteren Verschlechterungen der Rechtspositionen zugestimmt wird."[27]

(Bündnis 90/Die Grünen)

In der Bundesrepublik Deutschland bildet der Bundestag zusammen mit dem Bundesrat als Vertretung der Bundesländer die Legislative. Die Verlagerung von Gesetzgebungsbefugnissen auf die Europäische Union bedeutet einen teilweisen Einflussverlust für den Deutschen Bundestag. Einige Kritiker sehen darin gleichzeitig eine Schwächung der demokratischen Rückkopplung der Rechtsetzung, da sie der Europäischen Union ein Demokratiedefizit attestieren.[28] Dies gilt auch für den Wechsel von der Datenschutzrichtlinie zur Datenschutz-Grundverordnung. Wo eine europäische Richtlinie noch ein nationales Umsetzungsgesetz erfordert, bei dem ein gewisser Umsetzungsspielraum verbleibt, gilt eine europäische Verordnung direkt und ohne Umsetzungsakt in den Mitgliedstaaten. Die endgültige Fassung der Datenschutz-Grundverordnung enthält jedoch zahlreiche Öffnungsklauseln. Diese ermöglichen es den Mitgliedstaaten in bestimmten Bereichen eigene Vorschriften beizubehalten oder zu erlassen, sodass der

29 Bundesrat 2012.

Wechsel vom Instrument der Richtlinie zur Verordnung abgemildert wird. Anzahl und Reichweite der Öffnungsklauseln sind jedoch höchst umstritten. Eine indirekte Beteiligung aller zur Zeit der Aushandlungen der Datenschutz-Grundverordnung im Deutschen Bundestag vertretenen Parteien (CDU, CSU, SPD, Die Linke, und Bündnis 90/Die Grünen) ergab sich über das Europäische Parlament, dem wiederum Mitglieder der im Deutschen Bundestag vertretenen Parteien angehören.

Bundesländer

„Der Bundesrat hat heute eine Subsidiaritätsrüge gegen den Verordnungsvorschlag erhoben, mit dem die europäische Kommission einen neuen Rechtsrahmen zum Schutz personenbezogener Daten schaffen möchte. Der Vorschlag lege nicht ausreichend dar, warum eine verbindliche Vollregelung des Datenschutzes auf europäischer Ebene erforderlich sein soll. Zudem führe er mit seinem umfassenden verbindlichen Geltungsanspruch zur nahezu vollständigen Verdrängung mitgliedstaatlichen Datenschutzes und gehe weit über die Kompetenzzuweisung der EU hinaus. Er widerspreche damit den Prinzipien der Subsidiarität und Verhältnismäßigkeit (…)"[29]

(Bundesrat)

30 BVDW e. V. 2013.

Aufgrund der föderalen Struktur der Bundesrepublik Deutschland existieren in allen Bundesländern eigene Landesdatenschutzgesetze, die den Umgang mit personenbezogenen Daten durch die öffentliche Verwaltung regeln. Daneben existieren weitere landesspezifische Spezialgesetze zum Datenschutz. Auch diese Gesetze sind vom Erlass der Datenschutz-Grundverordnung betroffen und müssen bis zum Geltungsbeginn der Verordnung im Mai 2018 überarbeitet und angepasst werden.

Über den Bundesrat können die Landesregierungen Einfluss auf den Gesetzgebungsprozess auf Bundesebene nehmen. Anfänglich äußerte sich der Bundesrat kritisch zur Verordnung und sah darin eine Kompetenzüberschreitung des europäischen Gesetzgebers. Auch im weiteren Verfahren setzte er sich immer wieder für nationale Spielräume bei der Ausgestaltung des Datenschutzrechts ein.

Deutsches Recht

„Anstatt Unternehmen, wie bisher, mit einer Vielzahl verschiedener Gesetze, mit teils unzureichender Passgenauigkeit und Konkretisierung, zu konfrontieren, kann die EU-Datenschutzverordnung ein einheitliches Regelwerk für alle betroffenen Märkte schaffen. Hier kann die deutsche Gesetzgebung als Vorbild dienen, da diese, trotz historisch bedingter fehlender Berücksichtigung digitaler Medien, bereits ein selbstbestimmtes Verständnis von Datenschutz geschaffen hat. Dabei ist insbesondere der Wahrnehmung entgegenzutreten, deutsche Datenschutzstandards würden den Einsatz moderner Marketinginstrumente wie Personalisierung, Profilierung und Tracking verbieten und damit einen generellen Nachteil schaffen. Denn grundsätzlich dürfen deutsche Unternehmen das Gleiche wie Unternehmen in den USA – mit dem Unterschied, dass sie hierzu eine wirksame Einwilligung des jeweils betroffenen Nutzers einholen müssen, wenn sie personenbezogene Daten verwenden."[30]

(Bundesverband Digitale Wirtschaft e. V.)

31 In Deutschland erfolgte die Umsetzung allerdings erst im Jahr 2001.

32 Vgl. hierzu ausführlich Roßnagel 2017: S. 67 ff.

Das deutsche Datenschutzrecht wurde von vielen Akteuren gerade innerhalb der Diskussionen in Deutschland als ein „best practice Beispiel" hochgehalten und als Vorbild für die Datenschutz-Grundverordnung propagiert. Dieses setzt sich aus dem Verfassungsrecht und verschiedenen einfachgesetzlichen Vorschriften (Bundesdatenschutzgesetz, Telemediengesetz, Telekommunikationsgesetz sowie weiteren bereichsspezifischen Vorschriften) zusammen. Wenn von den Vorzügen des deutschen Datenschutzes die Rede ist, wird insbesondere die Errungenschaft des Rechts auf informationelle Selbstbestimmung, welches das Bundesverfassungsgericht im Jahr 1983 aus Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 Grundgesetz hergeleitet hat, hervorgehoben. Dieses gibt jedem das Recht, grundsätzlich selbst über die Preisgabe und Verwendung seiner Daten zu bestimmen. Auf diese Weise soll den Veränderungen und neuen Risiken der Informations- und Kommunikationstechnologien entgegengewirkt werden.

Das deutsche Datenschutzrecht wurde zum Teil von europäischen Vorgaben geprägt, hat diese aber auch selbst beeinflusst. Die EU-Datenschutzrichtlinie trat im Jahr 1995 in Kraft und musste in den folgenden drei Jahren von den europäischen Mitgliedstaaten in nationales Recht umgesetzt werden.[31] Die Verordnung wird mit ihrem Geltungsbeginn die EU-Datenschutzrichtlinie ablösen. Das Unionsrecht und das deutsche Datenschutzrecht gelten dann nebeneinander, da die Europäische Union keine Kompetenz besitzt, deutsche Gesetze außer Kraft zu setzen. Grundsätzlich haben EU-Verordnungen somit keinen Geltungsvorrang gegenüber den nationalen Gesetzen, auch wenn sie für die europäischen Mitgliedstaaten verbindlich sind. Hinzu kommt, dass sich in der Datenschutz-Grundverordnung zahlreiche Öffnungsklauseln finden, die es den europäischen Mitgliedstaaten ermöglichen, eigene Regelungen in bestimmten datenschutzrechtlichen Bereichen zu schaffen. Dadurch entsteht eine unübersichtliche Rechtslage, bei der sich Regelungen widersprechen können oder unklar ist, welche Vorschriften zur Anwendung kommen. In solchen Konfliktsituationen genießt das Unionsrecht daher einen Anwendungsvorrang gegenüber den nationalen Vorschriften. Das bedeutet, dass die Datenschutz-Grundverordnung zur Anwendung kommt und die entsprechenden innerstaatlichen Bestimmungen nicht angewandt werden dürfen.[32]

Vor diesem Hintergrund sind viele Anpassungen und Überarbeitungen des bestehenden deutschen Datenschutzrechts notwendig.

Denn obwohl die Verordnung nach ihrem Inkrafttreten im Mai 2018 unmittelbar ein Teil der Rechtsordnung jedes Mitgliedstaats wird, wird diese Wirkung durch viele Ausnahmeregelungen in der Verordnung eingeschränkt. Die Anpassung des nationalen Rechtsrahmens für den Datenschutz obliegt dem deutschen Gesetzgeber. Um dieser Aufgabe gerecht zu werden, muss er bestehende Vorschriften prüfen und gegebenenfalls neue Regelungen erlassen, um so die Lücken der Verordnung auszufüllen und die Vorschriften der Datenschutz-Grundverordnung unter Umständen zu ergänzen und zu präzisieren. Dies tut er beispielsweise durch die Schaffung eines neuen Bundesdatenschutzgesetzes. Dabei ist stets das Regelungsziel der Verordnung zu beachten und in der Durchsetzung zu unterstützen. Darüber hinaus sind die abstrakten und weit gefassten Regelungen der Verordnung in der Praxis sowohl durch den Europäischen Gerichtshof als auch durch nationale Gerichte und Aufsichtsbehörden zu konkretisieren.

Bundesverfassungsgericht

„Wer nicht mit hinreichender Sicherheit überschauen kann, welche ihn betreffenden Informationen in bestimmten Bereichen seiner sozialen Umwelt bekannt sind, und wer das Wissen möglicher Kommunikationspartner nicht einigermaßen abzuschätzen vermag, kann in seiner Freiheit wesentlich gehemmt werden, aus eigener Selbstbestimmung zu planen oder zu entscheiden."
(BVerfGE 65, 1 (43), 15.12.1983).

Das Bundesverfassungsgericht ist „Hüter des Grundgesetzes" und wacht über die Einhaltung deutscher Grundrechte. Im Jahr 1983 erkannte es in seinem Volkszählungsurteil[33] das Grundrecht auf informationelle Selbstbestimmung an, das seither den

33 BVerfG, Urt. v. 15.12.1983, Az. 1 BvR 209/83, 1 BvR 484/83, 1 BvR 440/83, 1 BvR 420/83, 1 BvR 362/83, 1 BvR 269/83.

34 BVerfGE 65, 1 (42).

35 BVerfGE 65, 1 (42).

grundrechtlichen Rahmen für die Verarbeitung personenbezogener Daten in der Bundesrepublik Deutschland bildet. Das Grundrecht „gewährleistet die Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen" und damit „selbst zu entscheiden, wann und innerhalb welcher Grenzen persönliche Lebenssachverhalte offenbart werden".[34]

Der Schutzbereich des Rechts auf informationelle Selbstbestimmung ist auf den Umgang mit personenbezogenen Daten beschränkt. Diese sind nach der Definition des § 3 Abs. 1 Bundesdatenschutzgesetz „Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person". Auf die Qualität des Datums kommt es dabei nicht an. Vielmehr stellte das Gericht schon im Jahr 1983 fest, dass es gerade durch den technischen Fortschritt und der damit verbundenen Möglichkeit des Sammelns und des Kombinierens von Daten „kein belangloses Datum" mehr gibt. Jede für sich gesehen noch so unerhebliche Information kann in Verknüpfung mit anderen Daten Rückschlüsse auf die Betroffenen, ihren Lebensweg und ihre Persönlichkeit ermöglichen. Einzelinformationen können so zu einem „weitgehend vollständigen Persönlichkeitsbild zusammengefügt werden".[35]

Ein Eingriff in das Recht auf informationelle Selbstbestimmung liegt in jeder fremdbestimmten Erhebung, Verarbeitung oder Nutzung personenbezogener Daten. Beschränkungen der informationellen Selbstbestimmung bedürfen einer „(verfassungsmäßigen) gesetzlichen Grundlage, aus der sich die Voraussetzungen und der Umfang der Beschränkungen klar und für den Bürger erkennbar ergeben und die damit dem rechtsstaatlichen Gebot der Normenklarheit entspricht".

Auf europäischer Ebene stehen dem Bundesverfassungsgericht der Europäische Gerichtshof und der Europäische Gerichtshof für Menschenrechte gegenüber, die über die Einhaltung der Charta der Grundrechte der Europäischen Union bzw. der Europäischen Menschenrechtskonvention wachen.

Irland
Irland spielt in der Datenschutzdebatte eine gewichtige Rolle. Viele datenverarbeitende Großkonzerne wie etwa Facebook Inc., Google Inc., Twitter Inc. und Microsoft Corporation haben das Land als Standort für ihre Niederlassungen und den Bau großer Datenzentren gewählt. Die Datenschutzaufsicht durch den Data Protection Commissioner of Ireland wurde indes als im europäischen Vergleich schwach wahrgenommen. Neben der geringen Personalausstattung herrschte darüber hinaus eine bezogen auf die Umstände der Datenverarbeitung im Vergleich zu Deutschland und den meisten EU-Mitgliedstaaten deutlich großzügigere Mentalität vor. Irland stand deshalb im Kern der Debatte um das sogenannte „Forum Shopping", einer Praxis, bei der ein Unternehmen bewusst die Staaten mit den niedrigsten – in diesem Kontext datenschutzrechtlichen – Beschränkungen als Sitz seiner Niederlassungen wählt; ein vor allem im Kontext von Steuervermeidung bekanntes Vorgehen (sog. Treaty Shopping). Die Datenschutz-Grundverordnung ist unter anderem mit dem erklärten Ziel angetreten, das Forum Shopping zu beenden.

Vereinigtes Königreich
Das Vereinigte Königreich hat infolge eines am 23. Juni 2016 abgehaltenen, nicht bindenden Referendums seinen Willen zum Austritt aus der Europäischen Union erklärt. Dies wird sich auch auf den Datenschutz auswirken. Insbesondere bedeutet es, dass das Vereinigte Königreich nach erfolgtem Austritt nicht mehr direkt an europäisches Datenschutzrecht gebunden sein wird. Die euroskeptische Haltung Großbritanniens zeigte sich auch in deren Position während der Verhandlungen um die Datenschutz-Grundverordnung. Großbritannien drängte immer wieder darauf die Verordnung in eine Richtlinie umzuwandeln und so größtmöglichen nationalen Spielraum zu bewahren.

36 Hogan Lovells 2012a.

USA

„Another concern we have is the regulation's requirement for explicit consent in all circumstances. We are concerned that a one-size-fits-all consent requirement would frustrate individual users because of the sheer number of consent requests they would be faced with, leading eventually to users just clicking through instead of making informed choices. At the same time, explicit consent can make it difficult for companies to use personal data in innovative ways to offer better services to consumers.(…) Furthermore, in the financial sector context, the 'right to be forgotten' could also lead to moral hazard, where defaulting parties demand their credit histories be deleted, putting the European financial system at risk. We also have concerns about the very limited protection to the freedom of expression that the regulation offers."[36]
(William E. Kennard, US-Botschafter der Europäischen Union)

Die US-Regierung hat wiederholt versucht Einfluss auf die Verhandlungen der Datenschutz-Grundverordnung auszuüben und ihr Verständnis von Privatheit und Datenschutz in den Prozess einzubringen. Von den meisten Mitgliedstaaten der Europäischen Union unterscheiden sich die USA durch ein deutlich unterschiedliches Verständnis von Privacy und von Datenschutz. Der Begriff „Privacy" ist im Text der Verfassung der Vereinigten Staaten von Amerika und ihrer Zusätze nicht enthalten; Gleiches gilt für den Begriff „Private Life". Vielmehr finden sich einzelne Aspekte von Privatheit, die sich zu einem Schutz der Privatsphäre vor staatlichen Eingriffen summieren, in anderen Vorgaben. Als Auslöser für die Entwicklung

37 Warren/Brandeis 2012 [1890]: S. 755 f.

38 De Maizière 2016.

eines „Right to Privacy“ im amerikanischen Deliktsrecht gilt ein Artikel von Warren und Brandeis aus dem Jahr 1890. Die Autoren beklagten, die Presse übertrete „in every direction the obvious bounds of property and decency. Gossip is no longer the resource of the idle and the vicious, but has become a trade, which is pursued with industry“.[37]

Privacy wird vor allem von der sogenannten „Castle Doctrine“ her gedacht. Diese geht auf einen Ausspruch des englischen Rechtsgelehrten Coke aus dem Jahr 1628 zurück: „For a man’s house is his castle – et domus sua cuique est tutissimum refugium.“

Hieraus hat sich im Gegensatz zu Deutschland ein eigenes „Privacy Law“ herausgebildet, das vornehmlich mit personenbezogenen Daten befasst ist. Der Begriff „Privacy Law“ ist demnach häufig auf die Erhebung und Verwendung personenbezogener Daten reduziert, also „Information Privacy“. Daneben lassen sich jedoch noch die Bereiche „Bodily Privacy“, „Privacy of Communication“ und „Territorial Privacy“ identifizieren.

In besonders starkem Kontrast steht der Ansatz, das Sammeln und Speichern von Daten und die Zuordnung zu einem Pseudonym solle noch kein Eingriff in die Rechte der Bürger*innen sein, sondern erst das bedarfsorientierte „Anfassen“ der Daten etwa durch staatliche Behörden zur Verbrechensaufklärung.

Sicherheitsbehörden

„Wir brauchen eine Technologieoffensive. Wir müssen unsere Sicherheitsbehörden noch viel mehr als bisher technisch ertüchtigen. (…) Wir müssen uns auch technologisch weiterentwickeln, etwa beim Einsatz von Biometrie. (…)“[38]

(Thomas de Maizière, Bundesminister des Innern)

39 Geminn 2015: S. 546 f.

40 Leaking bezeichnet das Durchsickern von Informationen an ein Publikum, dem diese Informationen ursprünglich vorenthalten werden sollten.

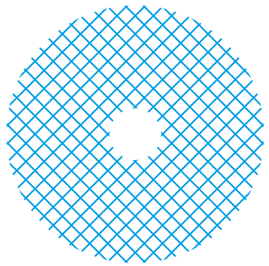
41 Beispielsweise die Weltbank, Google Inc., Yahoo Corporation, WikiLeaks, Unicef.

42 Beuth 2013.

43 Ebda.

Die Sicherheitsbehörden sammeln zur Erfüllung ihrer Aufgaben personenbezogene Daten und versuchen jede Art der elektronischen Kommunikation zu unterwandern. Dies führt jedoch zu einem Spannungsverhältnis zwischen dem Sicherheitsauftrag, den die Behörden haben, und den Interessen der Bürger*innen an ihrer Privatheit. Diese Problematik ist ursächlich für einen enormen Anstieg an verschlüsselten Internetverbindungen. Die Sicherheitsbehörden wünschen sich gesetzliche Ermächtigungsgrundlagen diese Verschlüsselungen aufheben oder den Einsatz von Hintertüren bei Verschlüsselungssystemen anwenden zu dürfen.[39]

Diese Praktiken der Geheimdienste gerieten in den letzten Jahren vermehrt in die öffentliche Kritik, nicht zuletzt aufgrund zahlreicher Leaks.[40] Im Juni 2013 begannen die Zeitungen „The Guardian“ und „The Washington Post“ geheime Dokumente zu veröffentlichen, die sie vom Whistleblower Edward Snowden erhalten hatten. Dies war der Beginn der sog. Snowden-Enthüllungen, die ein weltweites Netzwerk von Spionagesystemen vor allem rund um den Geheimdienst "National Security Agency" (NSA) und den britischen Geheimdienst „Government Communications Headquarters“ (GCHQ) aufdeckten. Klar ist, dass nicht nur namenhafte Firmen[41], zahlreiche Politiker*innen und Regierungschefs aus alle Welt ausgespäht wurden, sondern auch die normale Bevölkerung.[42] Es ging daher wohl auch um die eigenen wirtschaftlichen und politischen Interessen der ausführenden Länder.[43] Die Ausspähpraktiken insbesondere ausländischer Geheimdienste und die Möglichkeiten diese zu unterbinden, waren daher auch Thema in den Verhandlungen um die Datenschutz-Grundverordnung.



2.3. Die Welt des Datenschutzes

Die Welt des Datenschutzes versucht ein zuverlässiges und starkes Datenschutzniveau zu etablieren. Im Zentrum steht nicht der Schutz der Daten an sich, sondern der Schutz der Rechte des Einzelnen auf Privatheit und Selbstbestimmung als Voraussetzung für eine freie und offene Gesellschaft. Ein besonderes Anliegen der Welt des Datenschutzes ist deshalb der Ausgleich von Machtasymmetrien zwischen Individuen und Organisationen.

Wenngleich die unterschiedlichen Vertreter*innen der Welt ein gemeinsames Ziel verfolgen, so unterscheiden sie sich doch hinsichtlich des Mitteleinsatzes, um dieses Ziel zu erreichen, sowie

44 Für einen Überblick zur Rolle von Privatheit und Öffentlichkeit für die Demokratie siehe Geminn 2016: S. 601 ff.

45 EDRi 2012.

46 Vgl. etwa Digitalcourage e. V. o. J., Privacy International o. J. oder EDRi o. J.

hinsichtlich einer unterschiedlichen Rechtfertigungslogik. So macht es einen Unterschied, ob man institutionelle Mittel wie das Recht aktiviert (beispielsweise in Form von Klagen), oder ob man versucht durch öffentlichen Druck Veränderungen herbeizuführen. Der Schutz der Privatheit kann mit weiteren gesellschaftlichen Zielen verknüpft und als kollektives Gut betrachtet werden, das dem Wohle der Gemeinschaft dient (Bsp. Privatheit als Bedingung für Demokratie[44]). Privatheit kann ebenso als individuelle Angelegenheit betrachtet werden im Sinne eines persönlichen Anspruchs (Bsp. Autonomie des Individuums).

Datenschutzaktivist*innen

„Why we need a Regulation (and not a Directive): An EU wide, unified approach to securing an appropriately high level of data protection, and to the safeguarding of essential elements of democratic societies such as privacy and free speech is long overdue. It is crucial in a fast changing digital environment.“[45]

(European Digital Rights)

Die Datenschutzaktivist*innen möchten den Datenschutz stärken und die informationelle Selbstbestimmung des Einzelnen sowie Privatheit als Wert verteidigen. In der Rechtfertigung ihrer Tätigkeit wird dabei häufig auf höhere Werte Bezug genommen. Datenschutz ist demnach kein Selbstzweck, vielmehr setzt ihrer Meinung nach eine demokratische Gesellschaft zum Funktionieren und Überleben ein hohes Maß an informationeller Selbstbestimmung und an Privatheit als Bedingung voraus. Datenschutz wird nicht nur als individuelles Recht gesehen, sondern auch als gesellschaftlicher Wert wahrgenommen.[46] Die Datenschutz-Grundverordnung soll beides gewährleisten.

47 Lischka/Stöcker 2013.

48 EuGH, Urt. v. 06.10.2015, Az. C-362/14; ECLI:EU:C:2015:650.

Datenschutzaktivist*innen versuchen daher auf die Gesetzgebung einzuwirken sowie die Bevölkerung in Bezug auf datenschutzrechtliche Themen und Probleme zu sensibilisieren. Die Aktivist*innen orientieren sich dabei an Werten wie Freiheit, Transparenz und Rechtsstaatlichkeit. Zu ihren Praktiken zählen unter anderem öffentliche Stellungnahmen oder die Veröffentlichung von Leaks. Durch den Zusammenschluss von Interessengemeinschaften, Vereinen oder sonstigen Organisationen können sich Aktivist*innen mobilisieren und auf diese Weise ihre Rechtsposition erheblich verbessern sowie politischen Druck erzeugen. Bürger*innen können sich diesen Bündnissen anschließen oder diese in Form von Spenden oder Unterschriften unterstützen. Es gibt zahlreiche Zusammenschlüsse, die sich international für den Datenschutz einsetzen und versucht haben, bei den Verhandlungen um die Datenschutz-Grundverordnung Einfluss zu nehmen. Beispielhaft hierfür sind der Chaos Computer Club e. V. (CCC), Digitalcourage e. V., die Digitale Gesellschaft e. V., Privacy International, Article 19, Initiative für Netzfreiheit oder European Digital Rights. Während des Verhandlungsprozesses wurden insbesondere Forderungen nach einem starken Datenschutz, einer europäischen Harmonisierung und einheitlicher Durchsetzbarkeit des Datenschutzrechts sowie mehr Transparenz politischer Aushandlungsprozesse laut. Eine besonders tragende Rolle in den Verhandlungen nahm die Plattform Lobbyplag ein. Sie verfolgte den Gesetzgebungsprozess von Anfang an und veröffentlichte immer wieder interne Dokumente, die die Einflussnahme von Interessengruppen und insbesondere Wirtschaftsunternehmen auf die Verhandlungen transparent machen sollten. Diese Leaks bekamen insbesondere durch die mediale Berichterstattung Aufmerksamkeit in der breiten Öffentlichkeit.[47] Der Einfluss von politischen Aktivist*innen und die Verbreitung von Leaks kann zu weitreichenden Folgen für die gesamte Internetwirtschaft führen. Auch die Aufdeckungen von Edward Snowden machen diesen Effekt deutlich. So ist der Artikel 48 der Datenschutz-Grundverordnung, der die Vollstreckbarkeit und Anerkennung von Gerichts- und Verwaltungsbehördenentscheidungen von Drittländern behandelt, auf seine Enthüllungen zurückzuführen. Ein weiteres populäres Beispiel aus den Medien ist der Rechtsstreit[48] des österreichischen Juristen Maximilian Schrems gegen die irische Datenschutzbehörde, der bekannt wurde als Schrems vs. Facebook. Dieser führte dazu, dass der Europäische Gerichtshof das sog. „Safe Harbor-Abkommen“ mit den USA für ungültig erklärte.

49 BfDi o. J. a.

50 Zweiter Erwägungsgrund der Verordnung Nr. 45/2001 des Europäischen Parlaments und des Rates v. 18.12.2000 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Organe und Einrichtungen der Gemeinschaft und zum freien Datenverkehr, ABl. L 8/1.

51 Fox 2012.

52 Stupp 2015.

53 Datenschutzbeauftragter INFO 2014.

Datenschutzbehörden

„Beim Datenschutz geht es nicht um den Schutz von Daten. Im Mittelpunkt steht das informationelle Selbstbestimmungsrecht des Einzelnen und damit der Mensch.“[49]

(Andrea Voßhoff, Bundesbeauftragte für den Datenschutz und die Informationsfreiheit)

Datenschutzbehörden existieren sowohl auf europäischer (Europäischer Datenschutzbeauftragter) als auch auf nationaler Ebene (nationale Datenschutzbehörden). Die Behörden sind für die Einhaltung des geltenden Datenschutzrechts sowie bei Datenschutzrechtsverstößen für eine entsprechende Sanktionierung zuständig und laut Gesetz unabhängige Institutionen. Die Aufsichtsfunktion umfasst den Schutz der Datensubjekte vor unrechtmäßigen Zugriffen sowohl durch den Staat als auch durch Unternehmen. Die Behörden setzen Datenschutz mit Hilfe der Datenschutzgesetze und der Gerichte durch.

Der Europäische Datenschutzbeauftragte kontrolliert, ob alle Verarbeitungen durch die Organe und Einrichtungen der Europäischen Union das Recht auf den Schutz personenbezogener Daten achten.[50] Der bis zum Jahr 2014 amtierende Europäische Datenschutzbeauftragte Peter Hustinx bemängelte den Ausschluss von Polizei und gesetzlichen Autoritäten im Kommissionsentwurf zur Datenschutz-Grundverordnung, sprach sich aber auch dafür aus, mehr nationale Spielräume einzubauen.[51] Sein Nachfolger Giovanni Buttarelli kritisierte wiederum die Detailverliebtheit der drei Entwurfsversionen von EU-Kommission, Rat und Europäischem Parlament.[52] Sie seien nicht flexibel genug, um auf den künftigen technischen Wandel reagieren zu können.

Während der Europäische Datenschutzbeauftragte auf europäischer Ebene agiert, beschäftigt jeder Mitgliedstaat der Europäischen Union einen nationalen Datenschutzbeauftragten. Innerhalb Deutschlands hat jedes Bundesland einen Landesbeauftragten für den Datenschutz, der die öffentlichen Stellen des Landes im Bereich des Datenschutzes berät und überprüft. In den meisten Bundesländern ist er zugleich die zuständige Aufsichtsbehörde für nicht-öffentliche Stellen.[53]

54 Konferenz der Datenschutzbeauftragten des Bundes und der Länder 2015.

55 Büschemann 2015.

Die unabhängigen Datenschutzbehörden des Bundes und der Länder bilden als Zusammenschluss die sog. Datenschutzkonferenz. Der Zusammenschluss dient der Wahrung und dem Schutz der relevanten Grundrechte sowie dem Erreichen einer einheitlichen Anwendung des Datenschutzrechts innerhalb Deutschlands. Aus diesem Grund hat die Datenschutzkonferenz von Beginn an die Datenschutzreform um die Datenschutz-Grundverordnung mit dem Ziel unterstützt, einen modernen und stabilen Datenschutzrechtsrahmen für die Europäische Union bereitzustellen, ohne aber das derzeit herrschende Datenschutzniveau zu unterbieten. Dabei kritisierte sie besonders das Fehlen spezifischer Anforderungen zur Profilbildung oder der Videoüberwachung und mahnte bei den Verhandlungen die Autonomie des Einzelnen, die Transparenz und Zweckbindung bei der Datenverarbeitung sowie die Verantwortlichkeit der/des Datenverarbeitenden nicht außer Acht zu lassen.[54] Die institutionelle Anbindung der Datenschutzbehörden ermöglichte es ihnen, sich in den Verhandlungen um die Datenschutz-Grundverordnung Gehör zu verschaffen, schränkte aber gleichzeitig auch ihren Handlungsspielraum ein, indem es sie an institutionelle Routinen bindet. Vielfach mahnten die Datenschutzbehörden, die gesetzliche Durchsetzbarkeit von Gesetzen auch zu gewährleisten und die Behörden mit entsprechenden Ressourcen auszustatten, da Gesetze sonst wirkungslos blieben.[55] Gleichwohl existieren hinsichtlich der inhaltlichen Ausrichtung zwischen den einzelnen Datenschutzbehörden große Unterschiede. Während die irische Datenschutzbehörde regelmäßig mit dem Vorwurf konfrontiert wird, sehr wirtschaftsfreundlich zu agieren, gelten deutsche Datenschutzbehörden als weitaus datenschutzfreundlicher, wenngleich auch hier regionale Unterschiede bestehen.

56 vzbv 2012.

57 Vgl. etwa vzbv o. J. oder BEUC o. J.

Verbraucherschützer*innen

„Der Datenschutz ist vor allem durch die digitale Entwicklung zu einem immer wesentlicheren Teil des Verbraucherschutzes geworden. Eine Modernisierung ist dringend notwendig, um den Schutz der persönlichen Daten und die Privatsphäre der Verbraucher auch in Zukunft zu gewährleisten und gleichzeitig die Rechtssicherheit und Wettbewerbsfähigkeit der europäischen Unternehmen zu stärken."[56]
(Verbraucherzentrale Bundesverband e. V.)

Für Unternehmen werden Daten aufgrund der Digitalisierung zu einem immer wichtigeren Gut, sodass der Datenschutz auch in den Fokus des Verbraucherschutzes gerückt ist. Das Anliegen der Verbraucherschützer*innen ist es den Datenschutz zu stärken, um es den Verbraucher*innen zu ermöglichen, ihre Rechte besser zu wahren und um Wettbewerbsgleichheit zwischen den unterschiedlichen Akteuren auf dem Markt zu erreichen. Die Verbraucherschützer*innen vertreten die Interessen der Verbraucher*innen gegenüber Unternehmen und versuchen Chancengleichheit zwischen diesen herzustellen. Während der Verhandlungen veröffentlichten sie immer wieder Stellungnahmen und Kommentare.[57]

Die Verbraucher*innen sollen die Kontrolle über ihre Daten zurückgewinnen und ihre Autonomie gegenüber den Unternehmen behaupten. Innerhalb Deutschlands bündelt der gemeinnützige Verbraucherzentrale Bundesverband e. V. (vzbv) als Dachverband 16 Verbraucherzentralen der Länder und 25 verbraucherpolitische Verbände. Er klagt Verbraucherrechte vor Gericht ein und ist formell lediglich den Verbraucher*innen verpflichtet. Dabei fungiert er als eine Art Marktwächter, indem er Verbraucherprobleme aufzeigt, Lösungen anbietet und sich für deren Umsetzung einsetzt. Aufgrund des digitalen Wandels setzt sich der Verband darüber hinaus vermehrt für diejenigen Verbraucherrechte ein, die durch die Digitalisierung immer mehr an Bedeutung gewinnen. So

möchte er dazu beitragen, dass sich neue technische Innovationen im rechtlichen Rahmen bewegen, ohne dass Verbraucherrechte missachtet oder Innovationen gehemmt werden.

58 Richtlinie 95/46/EG des Europäischen Parlaments und des Rates v. 24.10.1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr, ABl. L 281/31.

59 BfDI o. J. b.

Artikel 29-Datenschutzgruppe

Die „Article 29 Working Party", die auch als „Artikel 29-Datenschutzgruppe" bezeichnet wird, wurde im Rahmen der Datenschutzrichtlinie[58] eingerichtet. Sie ist im Bereich des Datenschutzes das wichtigste Beratungsgremium der EU-Kommission bei der Zusammenarbeit mit den Mitgliedstaaten der Europäischen Union. Sie handelt in einer unabhängigen Beratungsfunktion und besteht aus einem/einer Vertreter*in der Kontrollstelle/n, die von jedem EU-Mitgliedstaat eingerichtet wird/werden, einem/einer Vertreter*in der Behörde/n, die für die EU-Institutionen und EU-Organe geschaffen wird/werden und einem/einer Vertreter*in der Europäischen Kommission. Innerhalb der Gruppe treffen die Datenschutzaufsichtsbehörden aller Mitgliedstaaten der Europäischen Union einen Konsens bezüglich verschiedener Datenschutzfragen und beraten dahingehend die EU-Kommission. Darüber hinaus hat die Arbeitsgruppe Expertenmeinungen bezüglich Fragen des Datenschutzes auf der Ebene der Mitgliedstaaten für die EU-Kommission bereitzustellen und eine einheitliche Auslegung der Datenschutzrichtlinie innerhalb aller europäischer Mitgliedstaaten sowie Norwegen, Liechtenstein und Island zu fördern. Ziel der Gruppe ist es, eine Harmonisierung des Datenschutzes innerhalb der Europäischen Union herbeizuführen.[59]

Während der Verhandlungen zur Datenschutz-Grundverordnung versuchte die Arbeitsgruppe durch Veröffentlichung von Dokumenten und Einschätzungen stets dazu beizutragen, dass ein hohes Datenschutzniveau innerhalb der Europäischen Union sichergestellt wird. Dabei legte sie besonderen Wert auf die Pseudonymisierung, den Schutz und die Stärkung der Rechte Betroffener, die Stärkung der Position der Aufsichtsbehörden sowie auf eine umfassende und aufgrund der technischen Möglichkeiten (z.B. technische Identifizierungsmöglichkeiten wie IP-Adressen) angemessene Definition des Begriffs „personenbezogene Daten". Auch wenn die Gruppe grundsätzlich eine positive Haltung gegenüber dem Vorhaben einnahm und besonders Aspekte wie das Recht auf Vergessenwerden, die Datenminimierung und die

60 BfDI 2012.

61 Erwägungsgrund 139 der Verordnung 2016/679 des Europäischen Parlaments und des Rates v. 27.04.2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung), ABl. L 119/1.

62 n-tv 2014.

63 Dabei ist es für die Einordnung zunächst unerheblich, ob es sich um personenbezogene Daten oder solche ohne Personenbezug handelt.

Vorschriften für die Verarbeitung von personenbezogenen Daten von Kindern lobte, hatte diese auch viele Kritikpunkte. So waren ihr einige Ausführungen der Verordnung nicht präzise genug. Sie betonte in diesem Zusammenhang die Wichtigkeit des Begriffs der „Einwilligung" und verbesserter Schutzmechanismen für die Betroffenen. Auch bei den Trilog-Verhandlungen nahm die Artikel 29-Datenschutzgruppe ihre Beratungsaufgaben wahr. So wünschte sie sich klare, einfache und effektive Lösungen, die zum einen den Betroffenen einen hohen Schutz ihrer Daten ermöglichen, aber zum anderen auch die Unternehmen nicht im Wettbewerb und im Kampf um Innovationen hemmen.[60]

Im Zuge des Geltungsbeginns der Datenschutz-Grundverordnung wird die Datenschutzrichtlinie zum 25. Mai 2018 aufgehoben und die Artikel 29-Datenschutzgruppe durch den Europäischen Datenschutzausschuss ersetzt.[61]

2.4. Die Welt der Digitalwirtschaft

„Noch vor Straßenbau und noch vor Schienenwegebau ist nichts so sinnvoll wie die Modernisierung der Energie- und der ICT-Infrastruktur (Anm. d. Verf.: information and communication technology)."[62]

(Günther Oettinger, EU-Kommissar für die digitale Wirtschaft und Gesellschaft)

Die Welt der Digitalwirtschaft betreibt Geschäftsmodelle, die auf den Umgang mit Daten angewiesen sind. Dies umfasst sowohl Unternehmen, deren Kerngeschäft auf dem Sammeln oder der Verarbeitung von Daten basiert[63] (Bsp. Google Inc., Facebook Inc.) als auch Unternehmen, die täglich eine große Menge an Daten verarbeiten, um einen reibungslosen Geschäftsvorgang zu gewährleisten, deren Kerntätigkeiten jedoch nicht datengetrieben sind (Bsp. Finanzbranche, Gesundheitswesen). Je nach Geschäftsmodell ergeben sich hierdurch unterschiedliche Interessen an Daten und Datenschutz. Während Datenschutz für datenbasierte

64 Vgl. etwa Bitkom 2015 oder DigitalEurope 2014.

65 DigitalEurope 2015.

Geschäftsmodelle häufig als hinderlich wahrgenommen wird, kann es für Bereiche wie die Telekommunikationsbranche oder den Finanzsektor essentiell sein ein hohes Datenschutzniveau einzuhalten, um das Vertrauen der Kund*innen nicht zu verlieren. Zudem mag es im Interesse der Unternehmen sein, das Gut „Daten" zu schützen, um die eigenen Geschäftsgeheimnisse zu bewahren. Dabei unterscheiden sich Unternehmensinteressen und -ziele nicht nur aufgrund unterschiedlicher Geschäftsmodelle, sondern häufig auch aufgrund der Unternehmensgröße oder des jeweiligen Standortes. Gemein ist jedoch allen, dass Datenschutz insbesondere dann eine Rolle spielt, wenn er den übergeordneten Geschäftsinteressen dient. In den Verhandlungen propagierten viele Vertreter*innen der Welt der Digitalwirtschaft immer wieder die zukunftsweisenden Verheißungen digitaler Technologien für die Wirtschaft.[64]

Europäische Unternehmen

„Europe needs a data protection regulation that allows it to embrace the data-driven innovations that are helping transform the economy, while at the same time granting enough protection to personal data to ensure that citizens trust the technologies."[65]

(DigitalEurope)

Im globalen Wettbewerb nimmt die Europäische Union in der Digitalwirtschaft eine vergleichsweise untergeordnete Rolle ein. Europäische Unternehmen der Informations-, Kommunikations-, Software- und Internetbranche bleiben in einigen Bereichen deutlich hinter Firmen aus den USA oder China zurück. Dies führt zu einer gewissen Abhängigkeit Europas in diesen Bereichen. Datenschutz wird durch europäische Unternehmen deshalb sehr zwiegespalten wahrgenommen. Einerseits erhoffen sie sich durch ein gewisses Datenschutzniveau das Kundenvertrauen zu stärken und potentielle Wettbewerbsvorteile gegenüber außereuropäischen Unternehmen zu gewinnen. Andererseits werden immer wieder

66 DigitalEurope 2014.

67 BVMW 2014.

Stimmen laut, die ein zu hohes Datenschutzniveau als Bedrohung für Innovation und Wachstum betrachten. Um im internationalen Vergleich bestehen zu können und eine größere Unabhängigkeit herbeizuführen, fordern Vertreter*innen aus der Wirtschaft daher in erster Linie seitens der Politik eine deutliche Stärkung des Handels im digitalen Bereich. Europäische Unternehmen verlangen den Abbau von Kosten durch zu viel Bürokratie, die Förderung von Innovationsmöglichkeiten und die Wahrnehmung von Chancen durch Big Data.[66]

Deutsche Unternehmen

„Eine EU-weite Datenschutz-Grundverordnung (EU-DSGVO) bietet die große Chance, das Datenschutzrecht in Europa umfassend zu modernisieren und zu harmonisieren und damit den europäischen Binnenmarkt zu stärken. (...) Der vorliegende Entwurf bedarf jedoch einer Mittelstandsklausel, damit der europäische Mittelstand im internationalen Wettbewerb bestehen kann. Die überwiegend mittelständisch geprägte Digitale Wirtschaft in Deutschland braucht eine verfügbare und leistungsfähige IT-Infrastruktur sowie eine nachhaltige Datenpolitik, um einen verantwortungsvollen Umgang mit Daten zu ermöglichen und global konkurrenzfähig zu sein."[67]

(Bundesverband mittelständische Wirtschaft)

68 BMWi 2015: S. 7.

69 Menz 2016.

70 BVMW 2014.

Deutschland bildet im internationalen Vergleich den fünftgrößten Markt in der Informations- und Kommunikationstechnologie-Branche – hinter den USA, China, Japan und Großbritannien.[68] Der rasante Fortschritt in diesem Bereich führt dazu, dass sich die Märkte und Marktstrukturen sehr schnell verändern und neue Marktführer die Digitalwirtschaft erobern. Einige Unternehmen sehen deshalb in strengen Datenschutzvorschriften vor allem einen Wettbewerbsnachteil gegenüber US-Unternehmen.

„Bevor wir uns der Schaffung neuer Regularien zuwenden, sollten zunächst die bestehenden gesetzlichen Regelungen genutzt und im Einzelfall – wenn nötig – an die veränderten Gegebenheiten der digitalen Welt angepasst werden. Aus unserer Sicht bremst eine weitere Regulierung vor allem Innovationen in Deutschland und Europa, fördert damit Rechtsunsicherheit und Bürokratie für junge und unerfahrene Start-ups und schafft so letztlich Markteintrittsbarrieren."[69]

(Zalando SE)

Aufgrund der schnellen konzeptionellen aber auch rechtlichen Veränderungen wird sich die deutsche Digitalwirtschaft permanent neu justieren müssen. Insbesondere die in Deutschland besonders vertretenen kleinen und mittelständischen Unternehmen fürchten die im Zuge der Datenschutz-Grundverordnung auf sie zukommenden Änderungen und die aus den notwendigen Umstellungen resultierenden Kosten. Daher setzten sie sich während der Verhandlungen für weniger Bürokratisierung ein.[70]

71 Schmiechen 2015.

72 Ebbinghaus/Schulz/Thiel 2014.

US-Unternehmen

„Das Internet hat uns gehört. Unsere Firmen haben es gebaut, verbreitet und perfektioniert, so dass andere nicht mithalten können. Und hinter den intellektuellen Positionen der Kritiker steckt das Interesse, diesen kommerziellen Erfolg auszuhöhlen. Zur Verteidigung von Google und Facebook muss man sagen, dass die europäische Reaktion manchmal mehr wirtschaftsgetrieben ist als alles andere."[71]

(Barack Obama, früherer US-Präsident)

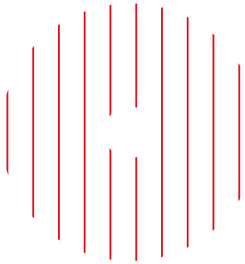
Die USA sind Heimat der bedeutendsten datenverarbeitenden Unternehmen der Welt. Insbesondere das kalifornische Silicon Valley gilt als Herz der Computer- und Softwareindustrie. Hier haben Firmen wie Facebook Inc., Hewlett Packard Inc., Apple Inc., Google Inc. und dessen Holding Alphabet Inc. und viele weitere ihren Sitz. Die amerikanischen Unternehmen prägen und dominieren die Digitalwirtschaft und nehmen eine überlegene Position auf dem digitalen Markt ein.

Nicht wenige dieser Unternehmen fokussieren sich auf datengetriebene Geschäftsmodelle. Sie sammeln, speichern und verkaufen personenbezogene Daten, indem sie sie zu einem handelbaren und kostbaren Gut erheben. Mittlerweile gelten personenbezogene Daten als „Rohstoff" des 21. Jahrhunderts.

Amerikanische Unternehmen versuchten während der Verhandlung um die Datenschutz-Grundverordnung durch gezielte Lobbyarbeit das Datenschutzniveau zu schwächen und setzten sich für Selbstregulierungsmaßnahmen ein.[72] Sie fürchteten erhebliche Nachteile, wenn sie sich auf ein höheres Datenschutzniveau einstellen müssen, da ihre Geschäftsmodelle und Angebote zum Teil mit den Grundprinzipien des Datenschutzes kollidieren.

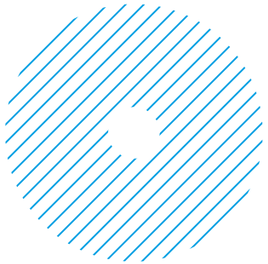
73 Rat der Europäischen Union, Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Datenschutz-Grundverordnung), 2012/0011 (COD) v. 11.06.2015.

74 Roßnagel 2016; siehe hierzu genauer: Richter 2015: S. 735; Roßnagel/Nebel/Richter 2015: S. 455.



2.5. Die Welt der Nachrichtenportale

Nachrichtenportale sind an der Herstellung von Öffentlichkeit beteiligt und berichteten regelmäßig über die Verhandlungen zur Datenschutz-Grundverordnung. Das Medien-Echo zur Datenschutz-Grundverordnung ist deshalb nicht nur nach ihrem Inkrafttreten enorm. Denn bereits während der Einigungsgespräche der EU-Organe zur Verordnung und nach der Veröffentlichung der finalen Version war das mediale Interesse an den Neuerungen des europäischen Datenschutzrechts groß. Die Nachrichtenportale bilden eine Art Schnittstelle zwischen den Bürger*innen und dem politischen Entscheidungsprozess und wirken als Vermittler. Sie informieren die Bevölkerung über die aktuellen Entwicklungen und die einzelnen Ergebnisse der Verhandlungsprozesse zur Datenschutz-Grundverordnung. Diese Berichte können den Bürger*innen wiederum als Informationsgrundlage dienen. Auf diese Weise haben Nachrichtenportale aber auch selbst Einfluss auf die Debatte um die Grundverordnung nehmen können. So wurde beispielsweise durch die mediale Berichterstattung nach dem Ratsentwurf[73] der Europäischen Union der Eindruck vermittelt, dass die Verordnung den Grundsatz der Zweckbindung aufweichen wolle.[74] Indem Nachrichtenportale mobilisiert werden, kann eine rechtliche Debatte angestoßen und ein Gesetzgebungsverfahren vorangetrieben werden. Die Welt der Nachrichtenportale griff insbesondere die Leaks der Datenschutzaktivist*innen zu den Lobbyvorgängen während der Verhandlungen in ihrer Berichterstattung auf.



2.6. Die Welt der Wissenschaft

Als kritisch-distanzierter Beobachter setzte sich die Welt der Wissenschaft während der Verhandlungen mit den Wechselwirkungen von Privatheit, Technik und Gesellschaft auseinander. Gleichzeitig ist die Wissenschaft in ihrer Forschungspraxis häufig auf personenbezogene Daten angewiesen und so selbst von der Datenschutz-Grundverordnung betroffen. Schließlich formen die Wissenschaften durch technische Entwicklungen den Rahmen, in dem Datenverarbeitung stattfindet, mit. Die Welt der Wissenschaft wird so auf vielfältige Weise selbst zum Teil der Arena.

Nicht zuletzt trägt das hier vorgestellte Projekt „Privacy-Arena" selbst dazu seinen Beitrag bei. Die Grenzen zwischen passiver Beobachtung und aktiver Teilnahme am Diskurs sind

75 „Jenseits der eigentlichen datenschutzrechtlichen Regulierung muss jedoch auch das Problembewusstsein der Nutzer berücksichtigt werden, wenn Fragen des Wettbewerbsvorteils diskutiert werden sollen: Insbesondere die Enthüllungen von Edward Snowden zum systematischen Zugriff von Nachrichtendiensten auf Internetdienste und internetbasierte Kommunikation haben zu einem spürbaren Vertrauensverlust der Nutzer geführt.", Oetjen 2016: S. 6.

76 „Wenn Grundprinzipien wie die Einwilligung und die Zweckbindung fallen würden, verlieren Verbraucherinnen und Verbraucher die Kontrolle über ihre eigenen Daten.", Müller 2015.

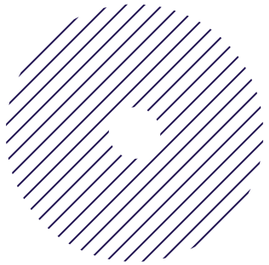
77 „Eine starke Datenschutzverordnung würde Bürgerinnen und Bürger wieder ins Zentrum der Onlinewirtschaft rücken.", Digitale Gesellschaft e. V. 2013.

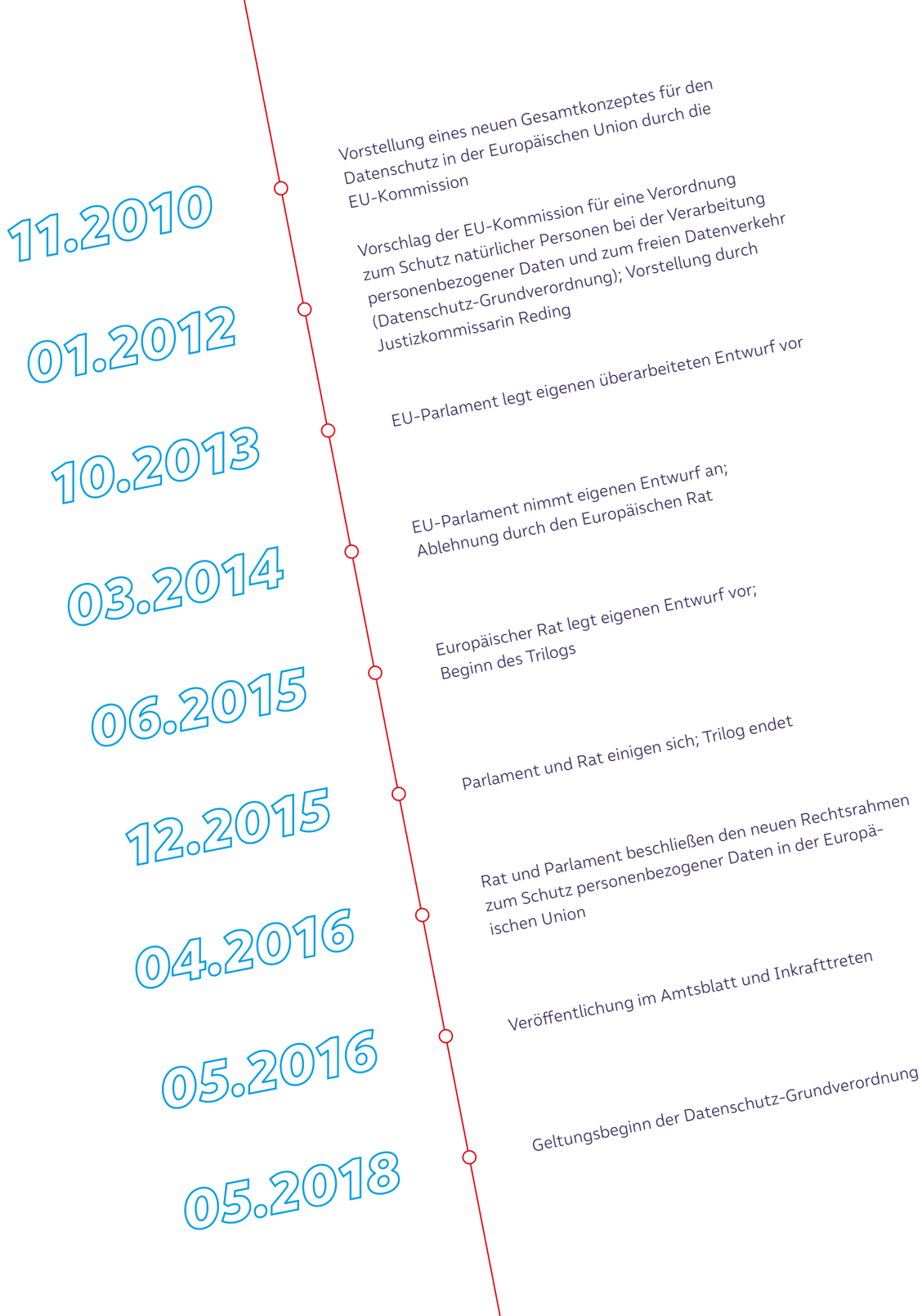
78 „Eine Datenverarbeitung darf darüber hinaus auch beim Nachweis der Notwendigkeit für das Verfolgen 'legitimer Interessen' erfolgen, allerdings nur unter der Voraussetzung, dass dadurch nicht die Grundrechte des 'Datensubjekts' unterwandert werden.", Verein Für soziales Leben e. V. o. J.

dabei stets fließend. Anstelle eine allwissende Objektivität zu beanspruchen, kann das Projekt vielmehr selbst als Teil der Arena betrachtet werden, welches versucht seine Geschichte der Datenschutz-Grundverordnung zu erzählen.

2.7. Die Welt der Nutzer*innen

In den datenschutzrechtlichen Debatten ist immer wieder die Rede von den Nutzer*innen[75], den Verbraucher*innen[76], den Bürger*innen[77] oder auch den Datensubjekten[78]. Gemeint sind damit all jene Personen, deren Daten beispielsweise bei der Nutzung von Informations- und Kommunikationstechniken, sozialen Netzwerken oder bei der Wahrnehmung verschiedener Dienstleistungen des Alltags erhoben, verarbeitet und genutzt werden. Sie nehmen in der datenschutzrechtlichen Diskussion eine Art Doppelrolle ein. Sie fungieren einerseits als Subjekte, die mit Rechten ausgestattet sind oder sein sollten. Andererseits sind ihre Daten und die von ihnen hinterlassenen Datenspuren aber auch selbst Waren oder wichtige Ressourcen und werden gehandelt. Entsprechend fordern die einen, das Vertrauen der Nutzer*innen oder Verbraucher*innen, das aufgrund von Datenskandalen erschüttert wurde, zurückzugewinnen, um weiterhin Zugang zu ihren Daten zu erhalten. Andere wiederum distanzieren sich von so einem instrumentellen Zugriff und verstehen den Schutz der Bürger*innen vor unrechtmäßigem Datenzugriff und Datenmissbrauch als notwendige Bedingung, um Demokratie zu gewährleisten oder die Autonomie der Individuen zu bewahren. Andererseits wird auch auf das ökonomische Potential der Datenverwertung hingewiesen sowie auf die Notwendigkeit, Zugang zu den Daten der Bürger*innen zu haben, um staatliche Kontrollfunktionen ausüben zu können. Dabei kommen die Datensubjekte selten selbst zu Wort, vielmehr sind sie zumeist Gegenstand der Verhandlungen, derer sich verschiedene Parteien bedienen.





3. Die Entwicklung der Verhandlungen im Zeitverlauf
Während der Verhandlungen rund um die Datenschutz-Grundverordnung bildeten sich verschiedene Konstellationen von Kompromissbildungen und Konfliktlinien zwischen den verschiedenen sozialen Welten sowie ihren Repräsentant*innen heraus. Manche dieser Verbindungen blieben konstant, andere veränderten sich im Zeitverlauf. Gelang es verschiedenen Welten ihre eigenen Interessen mit einem gemeinsamen Ziel zu verknüpfen, so entstanden Allianzen. Allianzen waren ein geeignetes Mittel, um die eigene Verhandlungsmacht in den Debatten zu stärken. Gleichzeitig gab es auch Konflikte, insbesondere dann, wenn sich die Interessen und alltäglichen Praktiken der Welten entgegenstanden. Im Folgenden sollen die Allianzen und Konflikte sowie ihre Veränderungen im Zeitverlauf dargestellt werden.

3.1 Die Arena formiert sich
In der Anfangsphase der Verhandlungen kristallisierten sich die zwei zentralen Konfliktlinien in der Arena heraus – der Konflikt zwischen der Welt der Digitalwirtschaft und der Welt des Datenschutzes sowie der zwischen der Welt der Nationalstaaten und der Welt der Europäischen Union.

Die starke Rolle der Europäischen Kommission im Kommissionsentwurf stößt auf Widerstand
Viele Elemente des im Jahr 2012 veröffentlichten Kommissionsentwurfs sahen eine Stärkung der EU-Kommission in ihrer Funktion vor. Die Kommission übernimmt in der Europäischen Union Exekutivaufgaben und ähnelt daher der nationalstaatlichen Regierung. Sie ist entsprechend daran interessiert, ihre eigenen Kompetenzen zu erweitern. Dies versuchte sie durch die Integration einer Vielzahl von delegierten Rechtsakten in die Datenschutz-Grundverordnung zu erreichen, die es der Kommission erlaubt hätten, unter Umgehung des Europäischen Parlaments und des Rates selbst unmittelbar Recht zu setzen. Bis auf zwei wurden diese Ermächtigungen der Kommission zum Erlass delegierter Rechtsakte im Laufe des Aushandlungsprozesses wieder entfernt.

Die Ausweitung der Souveränität der Europäischen Union führt zwangsläufig zu einem Souveränitätsverlust der Nationalstaaten und stößt auf entsprechenden Widerstand eben jener. Während sich für die Nationalstaaten wirtschaftliche Vorteile durch die transnationale Zusammenarbeit ergeben, ist dies aber auch immer mit einem Machtverlust auf nationaler politischer Ebene verbunden. Der Aufbruch nationalstaatlicher Rechtsräume zugunsten überstaatlicher Regularien wird deshalb insbesondere im Bereich öffentlicher Stellen von vielen Mitgliedstaaten der Europäischen Union kritisch beäugt. Einige forderten, dass die Regulierung staatlicher Datenverarbeitung im Vergleich zur privaten Datenverarbeitung unterschiedlich behandelt werde.

„Work on finding flexibility for the public sector related to Article 6(3) as well as to other parts of the draft regulation should be continued, on the understanding that it is only after this work that the assessment as to whether the regulation is capable of accommodating the required level of flexibility for member states' public sector can be made."[79]

(Pressemitteilung des 3228. Ratstreffens Justice and Home Affairs)

Darüber hinaus wird die starke Rolle der EU-Kommission auch von anderer Seite problematisiert. Der Entwurf sah einen Zuwachs an Kompetenzen der Kommission vor, insbesondere in Bereichen, die bisher den Datenschutzbehörden zugetragen wurden. Entsprechend kritisch äußerte sich die Artikel 29-Datenschutzgruppe gegenüber diesem Vorhaben und betonte die sich daraus ergebende Rechtsunsicherheit.[80]

79 Rat der Europäischen Union 2013.

80 „The Working Party has serious reservations with regard to the extent the commission is empowered to adopt delegated and implementing acts, which is especially relevant because a fundamental right is at stake. (…) The adoption of delegated or implementing acts for a large numbers of articles may take several years and could represent legal uncertainty.", Nielsen 2012.

81 Masing 2012.

82 BVerfGE 37, 271.

83 BVerfGE 73, 339.

Spannungen zwischen dem Europäischen Gerichtshof und dem Bundesverfassungsgericht

Die überragende Bedeutung von Datenverarbeitung in der modernen Gesellschaft brachte den deutschen Verfassungsrichter Masing dazu, vor einem „Abschied von den Grundrechten" zu warnen.[81] Hintergrund waren Ängste, dass mit dem Wechsel von der Richtlinie zur Verordnung deutsche Grundrechte marginalisiert werden. Insgesamt handelt es sich beim Datenschutzrecht um ein emotionales Thema in Deutschland, bei dem oft auf die lange und erfolgreiche Rechtstradition in Deutschland verwiesen wird. Die Datenschutz-Grundverordnung führe bezogen auf die Verarbeitung personenbezogener Daten zu einem Monopol des Europäischen Gerichtshofs in Fragen des Grundrechtsschutzes, jedoch handle es sich, so Masing, dabei um ein „Gericht ohne Unterbau" und um „kein Bürgergericht", das wie das Bundesverfassungsgericht von einzelnen Bürger*innen angerufen werden kann. Ein Äquivalent zur deutschen Verfassungsbeschwerde existiert nicht; einzelne Bürger*innen können nur indirekt Fälle vor den Europäischen Gerichtshof bringen. Zudem sei dieser angesichts der Zahl der zu erwartenden Verfahren unterbesetzt.

Ausgangspunkt dieser Befürchtungen sind die durch den Wechsel entstehenden Folgen für die Geltung nationaler Grundrechte. Deutsche Grundrechte etwa werden allenfalls noch dort relevant sein, wo die Datenschutz-Grundverordnung den Mitgliedstaaten Umsetzungsspielräume lässt. Diese fallen bei einer Verordnung deutlich enger aus als bei einer Richtlinie. Das grundlegende Verhältnis zwischen nationalen und europäischen Grundrechten hat das Bundesverfassungsgericht in seinen Solange-Entscheidungen[82] geklärt. Im Solange II-Urteil[83] heißt es: „Solange die Europäischen Gemeinschaften, insbesondere die Rechtsprechung des Gerichtshofs der Gemeinschaften einen wirksamen Schutz der Grundrechte gegenüber der Hoheitsgewalt der Gemeinschaften generell gewährleisten, der dem vom Grundgesetz als unabdingbar gebotenen Grundrechtsschutz im wesentlichen gleichzuachten ist, zumal den Wesensgehalt der Grundrechte generell verbürgt, wird das Bundesverfassungsgericht seine Gerichtsbarkeit über die Anwendbarkeit von abgeleitetem Gemeinschaftsrecht, das als Rechtsgrundlage für ein Verhalten deutscher Gerichte oder Behörden im Hoheitsbereich der Bundesrepublik Deutschland in Anspruch genommen wird, nicht mehr ausüben und dieses Recht mithin nicht mehr am Maßstab der Grundrechte des Grundgesetzes überprüfen."

Das Bundesverfassungsgericht beschränkt sich damit auf eine Art von „Mindestkontrolle“ dahingehend, ob durch die Europäische Union dem „Wesensgehalt der Grundrechte generell verbürgt“ wird. Dem steht der Anspruch des Europäischen Gerichtshofs gegenüber, umfassend und abschließend über Unionsrecht und dessen Anwendung zu entscheiden. Nach seinem weiten Verständnis gelten nationale Grundrechte nur, wenn keine Fallgestaltung denkbar ist, die vom Unionsrecht erfasst würde. Nach dem engen Verständnis des Bundesverfassungsgerichts kommt es indes darauf an, ob ein Sachverhalt unionsrechtlich determiniert ist. Das Verhältnis zwischen Europäischem Gerichtshof und Bundesverfassungsgericht war und ist also durchaus problembehaftet. Man kann von einer komplizierten und schwierigen „Kooperation“ oder „Kohabitation“ zwischen den beiden Gerichten sprechen. Praktische Auswirkungen hatten die Differenzen indes bisher nicht. Dies könnte sich durch die Datenschutz-Grundverordnung jedoch ändern.

Die Europäische Union rüstet sich gegen die Vormacht von US-Unternehmen

Der Konflikt zwischen den Souveränitätsansprüchen einzelner Länder und den Kompetenzerweiterungen der Europäischen Union entzündete sich auch an anderer Stelle. Mit der Datenschutz-Grundverordnung möchte die Europäische Union ihren Bürger*innen einen besseren Schutz ihrer Daten garantieren, wenn diese von US-Konzernen verwendet werden. Mit Hilfe der Verordnung wird ein einheitliches Datenschutzniveau innerhalb der Europäischen Union angestrebt, an welches sich im Sinne des Marktortprinzips auch amerikanische Konzerne halten müssen, die auf dem europäischen Markt aktiv sind. Gleichzeitig verfolgt die Europäische Union auch wirtschaftsprotektionistische Interessen. Die Verbesserung der Wettbewerbsbedingungen für europäische Unternehmen sowie die Förderung von Innovationen dient vor allem auch der Aufholjagd gegenüber amerikanischen Unternehmen, die in vielen Bereichen der Digitalökonomie der Europäischen Union weit voraus sind. Eines der Ziele der Europäischen Union ist es in der Digitalwirtschaft konkurrenzfähige IT-Unternehmen zu etablieren, die im globalen Wettbewerb mithalten können und die Europäische Union bei der Technologieführerschaft weiter vorantreiben. Auf diese Weise soll ein europäisches Gegengewicht geschaffen werden, das der Übermacht amerikanischer Konzerne entgegenwirkt.

84 Baker 2012.

85 O´Brien 2013.

86 Hogan Lovells 2012b.

87 EDRi 2013.

Die US-Regierung und die Digitalwirtschaft vereint im Kampf gegen den Datenschutz

Der US-Botschafter der Europäischen Union, William Kennard, forderte die Europäische Union dazu auf, der USA einen „adequate status" zuzuerkennen[84] und sprach sich für eine Rücknahme der ausdrücklichen Einwilligung bei einer Datenerhebung sowie des Rechts auf Vergessen aus.[85]

„Another concern we have is the regulation's requirement for explicit consent in all circumstances. We are concerned that a one-size-fits-all consent requirement would frustrate individual users because of the sheer number of consent requests they would be faced with, leading eventually to users just clicking through instead of making informed choices. At the same time, explicit consent can make it difficult for companies to use personal data in innovative ways to offer better services to consumers.(…) Furthermore, in the financial sector context, the 'right to be forgotten' could also lead to moral hazard, where defaulting parties demand their credit histories be deleted, putting the European financial system at risk. We also have concerns about the very limited protection to the freedom of expression that the regulation offers."[86]

(William E. Kennard)

In einem von der internationalen Bürgerrechtsvereinigung „European Digital Rights" veröffentlichten Schreiben der US-Regierung warnte diese die Europäische Union vor Handelshemmnissen und den terroristischen Gefahren, sollte der Datenaustausch zwischen den beiden Kontinenten durch die Grundverordnung zu sehr beeinträchtigt werden.[87] Die USA verfolgten dabei einerseits staatliche Interessen der Kontrollausübung. So sah eine Version im Vorfeld der Veröffentlichung des offiziellen Entwurfs der

88 Fox 2013.

89 „'I studied in Silicon Valley and there were companies coming to the classroom not knowing there is a European among them. They were saying it very bluntly: yes, Europe has strong data protection rules, but if you just pretend to respect them, you're fine. No way can they find out what we are doing on our servers and even if they do, it will take them at least 10 years to enforce anything.'(…) Schrems said.", Pop 2013.

90 Baker 2013.

EU-Kommission noch einen zusätzlichen Artikel vor, der es den USA erschwert hätte, Daten über Nutzer*innen von Unternehmen zu verlangen. Geleakte Dokumente konnten zeigen, dass dieser Artikel aufgrund intensiver Lobbyarbeit von Seiten der US-Regierung schließlich wieder gestrichen wurde.[88] Gleichzeitig verfolgte die US-Regierung auch wirtschaftliche Interessen. Gerade die Big Player der Digitalökonomie (z. B. Facebook Inc., Google Inc., u.a.) haben ihren Sitz in den USA. Ihre Monopolstellung aufzubrechen und europäische Konkurrenz zu befruchten, ist eines der Ziele der Datenschutz-Grundverordnung. Entsprechend erzeugte dies auf Seiten der US-Regierung und Teilen der Digitalökonomie Widerstand. Beide teilen das Interesse, die USA in ihrer wirtschaftlichen und politischen Stellung abzusichern. Gerade Unternehmen, deren Geschäftsmodelle datengetrieben sind, die aber nicht vom Vertrauen der Verbraucher*innen essentiell abhängig sind, da schlicht keine alternativen Konkurrenzangebote existieren, setzen sich für ein schwaches Datenschutzniveau ein und pochen auf Selbstregulierung.[89] Insbesondere amerikanische Technologiekonzerne haben durch Lobbyist*innen versucht, intensiv gegen unterschiedliche Bestimmungen der Datenschutz-Grundverordnung vorzugehen und Einfluss auf ihre Ausgestaltung zu nehmen, was zahlreiche geleakte Dokumente belegten.

Allerdings sind es nicht nur US-Unternehmen, die Datenschutz als Gefahr für datenbasierte Geschäftsmodelle betrachten. Auch europäische Unternehmen befürchten, dass ein zu enges Datenschutzgesetz Innovation und Wachstum in Europa schwächen könnte. Wenngleich Unternehmen, die Daten verarbeiten, aber deren Kerntätigkeit nicht datenbasiert ist (z.B. Unternehmen der Finanzbranche und des Gesundheitssektors), durchaus ein gewisses Interesse an Datenschutz haben, um das Vertrauen der Kunden nicht zu verlieren, so sind auch für sie strenge Regularien mit mehr Bürokratie und höheren Kosten verbunden. Europäische und amerikanische Unternehmen haben somit beide ein Interesse daran, dass Datenschutzniveau in der Europäischen Union zu schwächen.
Die Strategie der Wirtschaftsvertreter*innen umfasste auch die Errichtung eigener Organisationen, die auf den ersten Anschein wie NGOs oder gemeinnützige Vereine wirken (sollten). Dahinter verbergen sich Organisationen, die durch große Unternehmen finanziert werden und unter der Hand deren Interessen vertreten.[90] Im Bereich Privacy setzten sich diese Organisationen meist für ein moderates Maß an Datenschutz ein, solange es den eigentlichen Geschäftsinteressen der Unternehmen nicht im Wege stand.

91 Dehmel 2015.

Geschäftsmodelle der Digitalwirtschaft im Widerspruch mit den Grundprinzipien des Datenschutzes

Im Konflikt zwischen der Welt des Datenschutzes und der Welt der Digitalwirtschaft spiegelt sich eine der zentralen Streitlinien der gesamten Verhandlungen wider. Die Welt der Digitalwirtschaft fürchtet erhebliche Nachteile, wenn das Datenschutzniveau ihrer bisherigen Unternehmenspraxen angehoben werden muss, da deren Geschäftsmodelle und Angebote zum Teil mit den Grundprinzipien des Datenschutzes kollidieren. Datenschutz wurde von vielen Wirtschaftsvertreter*innen als Bedrohung für den wirtschaftlichen und gesellschaftlichen Wohlstand dargestellt.

„Die Datenschutzgrundverordnung sollte innovative Big Data Anwendungen fördern, anstatt diese zu bremsen. Big Data Analysen ermöglichen die Auswertung großer Datenmengen in hoher Geschwindigkeit und gelten als eine der wichtigsten Technologien der Zukunft. (…) Der weiteren Entwicklung von Big Data in Europa stehen sowohl das Gebot der Datensparsamkeit als auch die sogenannte Zweckbindung bei der Datenerhebung entgegen."[91]

(Susanne Dehmel, Mitglied der Geschäftsleitung Vertrauen und Sicherheit Bitkom e. V.)

92 Gesetz zur Verbesserung der zivilrechtlichen Durchsetzung von verbraucherschützenden Vorschriften des Datenschutzrechts v. 17.02.2016, BGBl. II, 233.

93 Vgl. § 3 Abs. 1 Satz 1 UKlaG.

94 Ackermann 2016.

95 BMJV 2015.

Für die Digitalwirtschaft stellen Daten vor allem eine Ware (z.B. Handel mit Daten für Werbezwecke) oder Nebenprodukte des alltäglichen Geschäftsablaufs dar (z.B. Kundendaten). Datenschutz spielt insofern eine Rolle, als er dazu dient, das Kundenvertrauen zu stärken oder die Daten des Unternehmens selbst vor fremden Zugriffen zu schützen. Jenseits dieser beiden Aspekte wird er oft als hinderlich wahrgenommen. Für die Welt des Datenschutzes stellt der Schutz personenbezogener Daten einen Teil der Kernpraktik der Welt dar, die mit bestimmten Werten und Zielen, wie dem Schutz der Rechte und Freiheiten des Einzelnen, verbunden ist. Somit ist Datenschutz nicht nur ein Instrument, um die eigene Kernpraktik auszuführen, vielmehr ist er selbst Bestandteil eben jener. Innerhalb der Welt des Datenschutzes rücken die einzelnen Vertreter*innen enger zusammen. So wird Datenschutz immer mehr ein Bestandteil des Verbraucherschutzes. Dies wird z.B. durch das Gesetz zur Verbesserung der zivilrechtlichen Durchsetzung von verbraucherschützenden Vorschriften des Datenschutzrechts[92] deutlich, wonach das Unterlassungsklagengesetz auf bestimmte Datenschutzrechtsverstöße durch Unternehmen erweitert wurde. Unternehmen verarbeiten zunehmend mehr Daten der Verbraucher*innen, ohne dass diese hierfür eine Einwilligung erteilt haben. Dies umfasst insbesondere die Datenverarbeitung für Werbung, Profiling oder den Adresshandel. Sofern ein Unternehmen gegen datenschutzrelevante Vorschriften verstößt, die dem Verbraucherschutz dienen, kann dieses auf Unterlassung in Anspruch genommen werden, da das Unterlassungsklagengesetz zum Tragen kommt. Den Anspruch können jedoch nicht die betroffenen Verbraucher*innen selbst geltend machen, sondern sie werden dabei durch Verbände oder Institutionen vertreten.[93] Auf diese Weise können die Verbraucherschutzzentralen tätig werden und das entsprechende Unternehmen verklagen oder abmahnen.[94] Hintergrund dieses Entschlusses ist der Wunsch, die Arbeit von Datenschutzbehörden durch den Rechtsschutz durch Verbraucherverbände zu ergänzen.[95] Der Bundesminister der Justiz und für Verbraucherschutz, Heiko Maas, sieht in der Ausweitung der Unterlassungsklage einen Erfolg:

96 Ebda.

„Das ist ein wichtiger Schritt zum besseren Schutz unserer Daten. Endlich bekommen Verbände bei Datenschutzverstößen ein Klagerecht. Personenbezogene Daten sind für den Wirtschaftsverkehr von unermesslicher Bedeutung. (…) Wir müssen uns darauf verlassen können, dass unsere Daten rechtlich geschützt sind und dieser Schutz auch durchgesetzt werden kann. (…) Alle darauf zu verweisen, ihre Recht einzeln einzuklagen, ist oft ein stumpfes Schwert. Viele trauen sich nicht, gegen große Unternehmen rechtlich vorzugehen. (…)“[96]

Auch wenn sowohl die Datenschützer*innen als auch Teile der Digitalwirtschaft ein Interesse an Datenschutz haben, können die dahinter liegenden Ziele somit teilweise konträr zueinander stehen. Während die Welt des Datenschutzes mit der Datenschutz-Grundverordnung vor allem die Rechte der Bürger*innen stärken möchte, geht es der Welt der Digitalwirtschaft um die Verbesserung der ökonomischen Ausgangslage.

3.2. Die Fronten verhärten sich

Im Laufe der Verhandlungen bildeten sich neue Bündnisse und Spannungen entlang der zentralen Konfliktlinien heraus. Ein Kompromiss oder eine Annäherung zwischen den unterschiedlichen Positionen der sozialen Welten und ihren Repräsentant*innen in der Arena schien in weite Ferne zu rücken.

97 Lobbyplag o. J. b..

98 Lobbyplag o. J. a.

99 Lischka/Stöcker 2013.

100 Initiative Data Protection in Europe 2013.

Allianz zwischen Datenschutzaktivist*innen und der Welt der Nachrichtenportale

Im Verlauf der Verhandlungen zur Datenschutz-Grundverordnung kam es immer wieder vereinzelt zu Leaks[97] von Dokumenten, die der Öffentlichkeit eigentlich nicht zugänglich gemacht werden sollten. Ins Zentrum der Aufmerksamkeit kamen diese Leaks vor allem durch ihre Thematisierung durch Nachrichtenportale. Datenschutzaktivist*innen konnten so Aufmerksamkeit für ihre Anliegen bekommen und Aufklärung betreiben. Gleichzeitig bot dies für die Welt der Nachrichtenportale die Gelegenheit, mit Hilfe eines Skandals Klickzahlen und Auflagen zu produzieren. Eine besonders tragende Rolle in den Verhandlungen nahm die Plattform Lobbyplag[98] ein. Sie verfolgte den Gesetzgebungsprozess von Anfang an und veröffentlichte immer wieder interne Dokumente, die die Einflussnahme von Interessengruppen und insbesondere Wirtschaftsunternehmen auf die Verhandlungen transparent machen sollten.

„Wie stark der konkrete Einfluss der Lobbyisten zuweilen ist, zeigt nun eine Internetplattform namens Lobbyplag: Sie dokumentiert in übersichtlicher Form, welche Abschnitte aus Papieren von Unternehmen und Lobby-Organisationen teils wörtlich in eine Stellungnahme des EU-Ausschusses für Binnenmarkt und Verbraucherschutz eingeflossen sind (…).“[99]

(Spiegel online)

Die Wissenschaft macht gegen die Lobbyindustrie mobil

Im Zuge des Bekanntwerdens der großflächigen Industrielobbyarbeit versammelten sich auch einige Wissenschaftler*innen um eine Gegenposition im öffentlichen Diskurs zu etablieren.[99] Wissenschaftler*innen aus ganz Europa starteten eine Onlinepetition und setzten sich für eine stärkere Regulierung des Datenschutzes ein, um zu verhindern, dass die Datenschutz-Grundverordnung aufgrund des enormen Lobbyeinflusses der Industrie verwässert wird. Zahlreiche Disziplinen, von den Rechtswissenschaften bis hin zu den Wirtschaftswissenschaften, unterzeichneten die Petition.

101 Nielsen 2013a.

102 Mitglied Bündnis 90/Die Grünen.

103 Tzschentke 2013.

104 BvD e. V. 2013.

105 Europäische Kommission 2013.

Uneinigkeit im Europäischen Parlament

Nach der Veröffentlichung des Kommissionsentwurfs nahm das Europäische Parlament seine Arbeit auf. Der Konflikt zwischen Datenschutz und Wirtschaftsinteressen spiegelte sich auch innerhalb des Europäischen Parlaments wider. Hier zeichnete sich eine Spaltung zwischen einer wirtschaftsfreundlichen (allen voran EPP, ALDE und ECR) und einer datenschutzaffinen (Grüne-EFA, GUE-NGL) Fraktion ab.[100] Der Europaabgeordnete Jan Philipp Albrecht[101] wurde vom Ausschuss für bürgerliche Freiheiten, Justiz und Inneres (LIBE) als zuständiger Berichterstatter ernannt. Seine Aufgabe bestand darin, sich federführend mit dem Kommissionsvorschlag auseinanderzusetzen und die Stellungnahme des Ausschusses vorzubereiten. Albrecht setzte sich öffentlich immer wieder für einen starken Datenschutz und einen offenen und transparenten Verhandlungsprozess ein.[102]

„Der Grundsatz muss heißen: im Zweifel für den Schutz der Person. Anders ist ein konsequenter Schutz auch nicht denkbar.“[104]

(Jan Philipp Albrecht, Abgeordneter des Europäischen Parlaments)

Albrecht bekam in seiner Position, die Grundrechte der europäischen Bürger*innen zu stärken und einen starken Datenschutz durchzusetzen, öffentliche Unterstützung von der damaligen Kommissionsvorsitzenden Viviane Reding.

„I am glad to see that the European Parliament rapporteurs are supporting the Commission’s aim to strengthen Europe’s data protection rules which currently date back to 1995 – pre-Internet age.“[105]

(Viviane Reding, damalige Vorsitzende der Europäischen Kommission)

106 So flossen Lobbytexte etwa von Amazon, Ebay und der US-amerikanischen Handelskammer in Anträge über gesetzliche Regelungen; vgl. Peters 2013.

107 So beispielsweise Änderungsvorschläge der Internet NGO Bits of Freedom, https://www.liberale.de/content/alvaro-gruene-datenschutzvorschlaege-fail.

108 Lischka/Stöcker 2013.

109 Pop 2013.

110 „'I can see a shift towards more of the protection, under quotation marks, of business interests and not the protection of citizen's fundamental rights.', Greek socialist MEP Dimitrios Droutsas told reporters in Brussels on Wednesday (15 May).", Nielsen 2013b.

111 Bergemann 2013.

Gleichzeitig übernahmen einige Parlamentarier*innen, wie diverse Leaks zeigten, teilweise wortgleich Forderungen von großen amerikanischen IT-Unternehmen, die die Schwächung einiger Datenschutzregeln forderten.[105] Lobbying wurde aber auch von verschiedenen Bürgerrechtsorganisationen betrieben, die versuchten ihre Forderungen nach einer datenschutzfreundlichen Reform in die Verhandlungen mit einzubringen. So fanden sich hier ebenfalls wortgleiche Übernahmen durch Parlamentarier*innen.[106] Die Anhörung verschiedener Interessengruppen zur Meinungsbildung ist kein ungewöhnlicher Prozess im europäischen Politikbetrieb, jedoch kritisierten viele Medien die Intransparenz des Verfahrens und das Übermaß an wirtschaftlicher Einflussnahme.[107]

„Lobbying is so intense and uneven on this law - Facebook alone has hired five lobbyists for this in Brussels, while on the other side, NGOs have maybe one person who also has to cover other topics too. And MEPs rarely go the extra mile of asking some independent experts or academics about it."[109]
(Maximilian Schrems, österreichischer Jurist und Datenschutzaktivist)

Insgesamt schienen sich zu diesem Zeitpunkt die Stimmen, die eine wirtschaftsfreundlichere Strategie verfolgten, im Parlament langsam durchzusetzen.[109]

Der Rat der Europäischen Union nähert sich der europäischen Digitalwirtschaft an

Nachdem das Europäische Parlament seine Stellungnahme veröffentlichte, nahm der Rat der Europäischen Union seine Arbeit auf und verhandelte unter Ausschluss der Öffentlichkeit über die Datenschutz-Grundverordnung. Dabei drangen nur wenige interne Informationen nach außen. Die Innen- und Justizminister*innen setzten vor allem auf den von der Ökonomie geforderten Ansatz der Selbstregulierung und den risikobasierten Ansatz. Generell schien der Rat eine unternehmensfreundliche Haltung einzunehmen.[110]

112 Industry coalition for data protection 2012.

Dem waren vielfache Warnungen europäischer Unternehmen vor den Folgen eines zu strengen Datenschutzes für den digitalen Binnenmarkt vorangegangen.

„However, the benefits of greater harmonisation are at risk of being outweighed by the costs of failing to strike the right balance between the protection of Europeans' fundamental right to privacy and data protection, and the promotion of innovation, competitiveness and growth in the Digital Single Market. If enacted in the present draft form, the Regulation would delay the launch of innovative services in Europe, cause substantial loss in revenues for businesses of all sizes and in a wide range of industries, limit opportunities for new market entrants, strongly increase administrative costs and create legal uncertainty."[112]
(Industry Coalition for Data Protection)

Sowohl im Rat als auch in der europäischen Digitalindustrie setzte sich die Ansicht durch, dass ein zu strenger Datenschutz schädlich für die Europäische Union sein könnte. Die Angst, abgehängt zu werden, langfristig nicht mit den Big Playern in den USA mithalten zu können und so in der Wirtschaft und dadurch letztendlich auch in der Politik zu einer marginalen Größe zu schrumpfen, bekräftigte diese Allianz.

113 Die Welt 2013.

114 Merkel 2013.

115 „Dank der Aufregung um Snowden konnten Datenschützer in den Entwurf sogar ein paar Punkte wieder hineinschreiben, die die Industrie bereits hatte streichen lassen.“, Biermann 2013.

116 Krempl 2013.

3.3. Datenschutz erfährt durch Snowden-Enthüllungen Aufschwung

Im Zuge der Snowden Enthüllungen erfuhr die Datenschutz-Grundverordnung vermehrt öffentliche Aufmerksamkeit. Wirtschaftsfreundliche Positionen zu Lasten des Datenschutzes verloren an öffentlicher Legitimität und Verter*innen dieser Positionen gerieten unter Druck sich neu zu positionieren.

Die Bundesregierung öffnet sich dem Datenschutz

Angela Merkel setzte sich als Reaktion auf den Snowden Skandal für den Schutz der Daten der Bürger*innen ein.[112] Ausländische Unternehmen und Regierungen wurden so kurzzeitig zu einem gemeinsamen Feind, vor dem es die „heimischen” Daten zu schützen galt.

„Wir arbeiten zusammen im Kampf gegen den Terror, aber auf der anderen Seite muss natürlich auch der Schutz der Daten der Bürgerinnen und Bürger gewährleistet sein. Nicht alles was technisch machbar ist, das wird ja in Zukunft immer mehr sein, darf auch gemacht werden.“[114]

(Angela Merkel)

Einigung im Europäischen Parlament zugunsten des Datenschutzes

Auch das Europäische Parlament blieb von den Snowden-Enthüllungen nicht unberührt. Die internen Streitigkeiten lösten sich kurzfristig auf und das Parlament trat geschlossen für ein schnelles Ende der Verhandlungen ein. Nach der Veröffentlichung des NSA-Skandals wurde Datenschutz zu einem brisanten Thema und stärkte die Verhandlungsposition der datenschutzfreundlicheren Kräfte innerhalb des Parlaments. Im Oktober 2013 konnte das Parlament eine gemeinsame Position verabschieden.[114] Es verfolgte das Ziel, die Verhandlungen mit den Mitgliedstaaten so schnell wie möglich zu beginnen.[115] Die Position des Parlaments machte gegenüber datenschutzfreundlichen Lösungen viele Zugeständnisse und näherte sich dem Anliegen vieler Vertreter*innen der Welt

117 Mit dem „One-Stop-Shop“ wird bei grenzüberschreitenden Datenverarbeitungen für Unternehmen und deren Tochtergesellschaften nur noch eine federführende Aufsichtsbehörde am Sitz der „Hauptniederlassung” zuständig sein, vgl. Art. 56 Abs. 1 DSGVO.

des Datenschutzes an, ein starkes Datenschutzniveau zum Wohle der Bürger*innen zu verankern.

3.4. Die Angst der Europäischen Union vor wirtschaftlicher Abhängigkeit

Die Mitgliedstaaten der Europäischen Union fürchteten nicht nur die politische Abhängigkeit, sondern auch den Verlust ihrer Wettbewerbsfähigkeit gegenüber amerikanischen IT-Großunternehmen. Wirtschaftsfreundliche Positionen wurden in der Arena wieder dominanter. Die Drohszenarien der Welt der Digitalwirtschaft vor den vermeintlich negativen Folgen durch einen zu hohen Datenschutz hatten ihre Wirkung entfaltet.

Der Kampf um Souveränität der Nationalstaaten

Gegen Ende des Jahres 2013 gerieten die Verhandlungen um die Datenschutz-Grundverordnung schließlich wieder ins Stocken. Im Rat der Europäischen Union, der sich als letztes Organ (nach Kommission und Parlament) auf eine gemeinsame Stellungnahme zur Verordnung einigen musste, bevor die aufgrund der wechselseitigen Ablehnung der jeweiligen Vorschläge zwischen Rat und Parlament notwendigen Trilogverhandlungen beginnen konnten, kam es immer wieder zu Verzögerungen. Insbesondere das Prinzip des One-Stop-Shop[116] führte wiederholt zu Konflikten zwischen den Mitgliedstaaten. Einzelne Länder, darunter das Vereinigte Königreich, Dänemark, Slowenien und Ungarn, lehnten eine Verordnung generell ab und plädierten für die Umwandlung in eine Richtlinie. Deutschland wiederum versuchte zu verhindern, dass der öffentliche Sektor ebenfalls von der Verordnung erfasst wird. Der Ursprung der zähen Verhandlungen lag in der Angst der einzelnen Staaten, in relevanten Bereichen Souveränität abgeben zu müssen.

Die Sorge der Bundesregierung um den nationalen wirtschaftlichen Wohlstand

Angela Merkel zweifelte öffentlich, ob Datenschutz als Oberziel zukunftsfähig ist. Vielmehr betonte sie die Wichtigkeit wirtschaftlicher Aspekte und trat für eine Stärkung der heimischen Industrie und im Zuge dessen für europäische Unternehmen ein.

118 Merkel 2015.

119 „Member states have since held protracted internal debates with signs suggesting that Germany is now leading the pack in rolling back key points in the original draft.", Nielsen 2015b.

„Wir müssen hohe Datensicherheit haben, aber wenn wir uns das Big Data Management, wenn wir uns die Möglichkeit der Verarbeitung großer Datenmengen durch einen falschen rechtlichen Rahmen zu sehr einengen, dann wird nicht mehr viel Wertschöpfung in Europa stattfinden. Das wäre für uns von großem Nachteil."[118]

(Angela Merkel)

Die deutsche Bundesregierung teilte somit die Interessen vieler europäischer Unternehmen, die im Datenschutz eine Gefahr für die Konkurrenzfähigkeit der europäischen Wirtschaft sahen. Als eine Vertreterin der Welt der Nationalstaaten handelt sie im Interesse Deutschlands. Gesellschaftlicher Wohlstand wird hier eng an den ökonomischen Wohlstand gekoppelt. Europäische Unternehmen wiederum verfolgen wirtschaftliche Interessen der Profitgenerierung und möchten ihre Wettbewerbsfähigkeit verbessern. Die Forderung datengetriebene Geschäftsmodelle zu ermöglichen und verstärkt auf Selbstregulierung zu setzen, kann somit die Interessen beider Welten vereinen.

Der Rat der Europäischen Union unter dem Einfluss europäischer Unternehmen

Im März 2015 wurden erneut Dokumente veröffentlicht, die eine enge Kooperation des Rats der Europäischen Union und der Digitalökonomie belegen sollten. Insbesondere Deutschland, welches eine maßgebliche Rolle in den Verhandlungen einnahm, näherte sich in seiner Position der Industrie an.[118] Beim direkten Vergleich der US-amerikanischen und europäischen Digitalwirtschaften wird häufig die Meinung vertreten, dass die Europäische Union durch den Datenschutz die internationale Wettbewerbsfähigkeit ihrer Unternehmen und die europäischen IT-Innovationen hemme, es zugleich aber auch nicht-europäischen Unternehmen erschwert werde innerhalb der Europäischen Union zu bestehen. Im Juni 2015 einigte sich der Rat schließlich und veröffentlichte seine

120 Nielsen 2015a.

Version eines Vorschlags für eine Datenschutz-Grundverordnung. Zahlreiche Datenschutz- und Verbraucherschutzorganisationen kritisieren die endgültige Ratsversion der Verordnung als zu wirtschaftsfreundlich. Einer der Hauptvorwürfe sind die vielen Schlupflöcher für Unternehmen, die es ihnen ermöglichen, die Daten ihrer Kunden auszuspähen.[119]

Da der ursprüngliche Entwurfsvorschlag der Europäischen Kommission aus dem Jahr 2012 sowohl vom Europäischen Parlament als auch dem Rat der Europäischen Union abgelehnt wurde und beide eigene Entwurfsversionen der Datenschutz-Grundverordnung vorschlugen, begannen Ende Juni 2015 die Trilogverhandlungen zwischen allen drei Parteien. Im Dezember 2015 einigten sich das Europäische Parlament, die Europäische Kommission und der Rat der Europäischen Union schließlich auf eine gemeinsame Fassung der Datenschutz-Grundverordnung. Dabei konnte sich der Rat in weiten Teilen mit seinen Vorstellungen durchsetzen.

4. Fazit

Die Verhandlungen um die Datenschutz-Grundverordnung waren äußerst vielschichtig. Es ging nicht nur um den Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, wie es Art. 1 der Datenschutz-Grundverordnung letztlich als Ziel der Verordnung vorgibt, sondern weit darüber hinaus. So wurde etwa mitverhandelt, welche Bedeutung Privatheit heute und in Zukunft haben soll und haben kann, und welche marktwirtschaftlichen Folgen die Verordnung für europäische Unternehmen haben wird. Außerdem wurden die Rechtsetzungsprozesse auf europäischer Ebene in den Blick genommen und teilweise stark kritisiert.

4.1 Privatheit und Datenschutz

Datenschutz steht in einer immer stärker vernetzten und digitalisierten Welt im Zentrum der Debatte um den Schutz von Privatheit und Selbstbestimmung. In den 1990er Jahren bildeten mit dem „Großen Lauschangriff" noch optische und akustische Überwachungsmaßnahmen den Schwerpunkt der Debatte um die Privatheit der eigenen Wohnung, während die Debatte um

Privatheit in öffentlichen Räumen von der Überwachungskamera dominiert war. Ängste bezogen auf Privatheit und Datenverarbeitung richteten sich vornehmlich gegen den Staat und führten in den 1980ern zu starkem Widerstand gegen eine geplante Volkszählung. Hier spielen nicht zuletzt die Erfahrungen der Deutschen im Nationalsozialismus und die zeitgenössische Wirklichkeit einer umfassenden Überwachung der eigenen Bevölkerung durch das Ministerium für Staatssicherheit in der DDR eine Rolle. Neu belebt wurden diese Ängste durch die Enthüllungen des Whistleblowers Edward Snowden, der die umfangreichen Abhör- und Datensammelaktivitäten anglo-amerikanischer Geheimdienste der breiten Öffentlichkeit bekannt machte. Daneben werden Daten aber vornehmlich von privaten Unternehmen erhoben und ausgewertet. Die Ziele sind hierbei vielfältig und reichen vom Anbieten personalisierter Werbung bis hin zur Marktforschung. Besonders greifbare Fokuspunkte der Debatte um Privatheit in einer digitalen Welt sind die Zulässigkeit von verschlüsselter Kommunikation ohne Hintertüren für Sicherheitsorgane und die anonyme Nutzung von Dienstleistungen und Kommunikationsplattformen im Internet. Staatliche und privatwirtschaftliche Interessen stehen hier, wie auch in vielen anderen Fällen, in direktem Widerstreit mit den Interessen der Bürger*innen.

Dies spiegelte sich auch in den Verhandlungen zur Datenschutz-Grundverordnung wider. Wenngleich nicht immer explizit Bezug zur Privatheit genommen wurde, fanden sich doch häufig implizite Bezüge, die Aufschluss über die unterschiedlichen Vorstellungen über Privatheit in der Arena gaben. So fanden sich einerseits individuelle Privatheitsvorstellungen, die Privatheit vor allem als Problem des Einzelnen ansehen. Privatheit wird als ein Aspekt unter vielen betrachtet, den es im unternehmerischen Handeln zu berücksichtigen gilt. Ihm wird aber kein übergeordneter Wert beigemessen. Er stellt lediglich einen Faktor unter vielen dar, der wahlweise hinderlich für den gesellschaftlichen Wohlstand sein kann (Bsp. Datenschutz als Innovationsbremse) oder als ein positiver Aspekt für die Geschäftsinteressen berücksichtigt wird (Bsp. Datenschutz als Wettbewerbsvorteil). In diesem Sinne wird der wirtschaftliche Wohlstand mit gesellschaftlichem Wohlstand gleichgesetzt und als dem Allgemeinwohl dienend gerahmt, während Privatheit letztendlich als persönliche Angelegenheit zu einem gewissen Grad auch abdingbar ist. Solche Bezüge finden sich häufig bei den Vertreter*innen wirtschaftsfreundlicher Positionen.

121 Ombudsman Europa 2016.

Privatheit kann aber auch selbst als ein kollektiver Wert betrachtet werden, der dem Allgemeinwohl dient. Als Voraussetzung für eine freie und offene Gesellschaft muss er demnach verteidigt und beschützt werden. Insbesondere Vertreter*innen datenschutzfreundlicher Positionen folgen tendenziell eher diesem Leitbild. Die einzelnen Welten bewegen sich stets innerhalb dieses Kontinuums.

In der Arena der Datenschutz-Grundverordnung geht es aber um mehr als nur um Datenschutz und Privatheit selbst. Mitverhandelt wurden auch immer bestimmte Vorstellungen, wie man die Gesellschaft gestalten kann. Seien es die Verheißungen vieler Ökonomen, die mit einem „Mehr" an Daten eine prosperierende Wirtschaft und letztendlich ein besseres Leben für die Gesellschaft propagierten. Oder Datenschützer*innen, die genau in dieser Technikgläubigkeit eine Gefahr sahen und gerade deshalb die Privatheit selbst als eine grundlegende Bedingungen für ein gutes und freies Leben betrachteten.

4.2. Die Verhandlungen über die Datenschutz-Grundverordnung zwischen Sichtbarkeit und Unsichtbarkeit

Zum Gegenstand der Verhandlungen wurde auch die Frage, wie die Aushandlungen selbst von statten gingen, und somit die Frage nach der Art und Weise politischer Entscheidungsprozesse. Immer wieder wurden Stimmen laut, die mehr Transparenz des Gesetzgebungsverfahrens forderten. Die Gesetzgebungsverfahren der Europäischen Union und insbesondere das Trilogverfahren stehen immer wieder in der Kritik, intransparent und undemokratisch zu sein. So kritisierte die Bürgerbeauftragte der Europäischen Union Emily O'Reilly:

„It is difficult to find out when trilogues are taking place, what is being discussed and by whom without a great deal of time and effort. (…) Making this information available should enable citizens to hold their representatives to account and to engage effectively in the legislative process."[121]

(Emily O'Reilly, Bürgerbeauftragte der Europäischen Union)

122 Vgl. Center for Democracy & Technology o. J. oder European Privacy Association o. J.

Insbesondere die intransparente Einflussnahme verschiedener Interessenvertreter*innen auf Politiker*innen wurde kritisiert. Die Lobby der Digitalökonomie versuchte in den Verhandlungen auf Hinterbühnen zu agieren und sich der öffentlichen Sichtbarkeit zu entziehen. Die Lobbyindustrie setzte dabei verschiedene Strategien ein. Zum einen wurde versucht, durch Gespräche mit Politiker*innen Einfluss auf den Prozess zu nehmen. Was zunächst keinen ungewöhnlichen Vorgang darstellt, wird jedoch dann problematisch, wenn es einen Überhang wirtschaftlicher Einflussnahme gibt. Durch das Abwerben von Personen mit zahlreichen Verbindungen in den Politikbetrieb wurde versucht, die Einflussnahme zu verstärken. Dies erfordert einen enormen Mitteleinsatz. Durch die im Vergleich zu zahlreichen Datenschutzorganisationen finanziell weitaus besser ausgestattete und gut vernetzte Lobbyindustrie kam es zu einem Ungleichgewicht der Einflussnahme. Zugleich wurden Selbstregulierungsmaßnahmen, sei es auf Seiten der Unternehmen oder auf Seiten der Verbraucher*innen, im Sinne von Selbstdatenschutz propagiert. Ebenso wurden ein Glaube an Technik und deren gesellschaftlichen Mehrwert sowie die Freiheit des Internets und die Autonomie des Individuums als Werte hervorgehoben.[121] Insbesondere die Intransparenz der zahlreichen Einflussnahmen unterläuft die institutionellen Mechanismen der demokratischen Entscheidungsfindung. Während die politischen Institutionen formell zu funktionieren scheinen, fallen die eigentlichen Entscheidungen hinter verschlossenen Türen. Wer gehört wird und wessen Stimmen zählen, folgt keinem geregelten Prozess, sondern hängt zu einem großen Teil von der Ausstattung mit Ressourcen ab. Es gibt aber auch Gegenbewegungen in der Arena. Einige Akteure stellten sich der Intransparenz des Gesetzgebungsverfahrens nicht nur auf diskursiver Ebene, sondern auch praktisch entgegen: Die Praktik des Leakings wurde benutzt, um öffentliche Sichtbarkeit zu erzeugen und verschiedene Akteure um den Gegenstand der Datenschutz-Grundverordnung zu versammeln.

Datenschützer*innen (insbesondere Aktivist*innen und Verbraucherschützer*innen) versuchten der Unsichtbarkeit im Aushandlungsprozess entgegen zu wirken. Sie plädierten in ihren Stellungnahmen immer wieder für mehr Transparenz in den Verhandlungen rund um die Datenschutz-Grundverordnung. Die Medienöffentlichkeit wurde als Ressource genutzt, nicht nur um öffentlichen Druck auf die Politiker*innen und Akteure der Digitalökonomie zu erzeugen, sondern auch um verschiedene Akteure

123 Leaks spielten in den Verhandlungen eine zentrale Rolle, dienten sie gerade für die Befürworter*innen eines starken Datenschutzes als Möglichkeit, Öffentlichkeit zu erzeugen, in der Debatte Gehör zu finden und die Routinen der Hinterzimmerpolitik kurzzeitig zu durchbrechen. Das Gesetzgebungsverfahren wurde dabei nicht an sich angezweifelt, sondern die Art und Weise, wie es ausgeführt wurde.

124 Vgl. Art. 83 DSGVO.

um das Verhandlungsobjekt der Datenschutz-Grundverordnung versammeln zu können, die sonst nicht Teil des Diskurses gewesen wären.[122] Der Hinweis auf interne Probleme demokratischer Verfahrensweisen war eine Art Korrekturversuch. Solch ein Modus hält nach wie vor an institutionellen Routinen fest, ist aber um interne Reformen bemüht. So zeigten sich in diesen Reaktionen in Zeiten digitaler Krisen letztendlich auch bestimmte Vorstellungen darüber, was Demokratie bedeuten kann.

5. Ausblick

Die Schwierigkeiten des Aushandlungsprozesses um die Datenschutz-Grundverordnung werden insofern im Ergebnis deutlich, als die Ziele der Verordnung nur teilweise erreicht wurden. Auf der einen Seite machen drakonische Sanktionen Druck auf Unternehmen, datenschutzrechtliche Vorgaben genau zu beachten. Zudem werden die Stellung der Datenschutzbeauftragten in der Europäischen Union verbessert und die Rechte und Beschwerdemöglichkeiten des Einzelnen gestärkt. Auf der anderen Seite werden jedoch konzeptionelle Probleme des Datenschutzrechts perpetuiert.

Ferner kommen durch die Datenschutz-Grundverordnung auf europäische Unternehmen viele neue rechtliche Herausforderungen zu. Diese sind mit Kosten und einem hohen Planungsaufwand verbunden. Sie führen in vielen Bereichen zu erheblichen Pflichten und zusätzlichen Belastungen wie der Datenschutz-Folgenabschätzung, mehr Dokumentations- und Informationspflichten sowie dem Recht der Verbraucher*innen auf Datenübertragbarkeit. In anderen Bereichen ist der Unterschied zur bisherigen datenschutzrechtlichen Praxis jedoch eher gering. Die höheren Bußgelder bei Verstößen gegen die Verordnung bergen für Unternehmen ein größeres wirtschaftliches Risiko.[123] Diesen Herausforderungen müssen sich aber nicht nur europäische Unternehmen stellen, sondern alle in der Europäischen Union agierenden Unternehmen. Dies ist auf die Einführung des Marktortprinzips zurückzuführen, welches vorsieht, dass das europäische Datenschutzrecht auch von Unternehmen aus dem EU-Ausland beachtet werden muss, wenn diese innerhalb der Europäischen Union personenbezogene Daten verarbeiten und nach Art. 3 Abs. 2 DSGVO entweder Dienstleistungen oder Waren innerhalb der Europäischen Union anbieten oder das Verhalten der betroffenen Person beobachten.

125 Entwurf eines Gesetzes zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680 (Datenschutz-Anpassungs- und -Umsetzungsgesetz EU - DSAnpUG-EU), BR-Drs. 110/17.

126 Öffnungsklauseln ermöglichen es den Mitgliedstaaten in bestimmten Bereichen eigene Vorschriften beizubehalten oder zu erlassen. Ihre Reichweite (und sogar ihre Existenz) ist jedoch Gegenstand einer intensiven Debatte.

127 Krempl 2017.

128 Roßnagel 2016.

Darüberhinaus sind konkrete Aussagen zur Implementierung der Datenschutz-Grundverordnung derzeit kaum möglich. Die Bundesregierung hat am 1. Februar 2017 den Entwurf eines neuen Bundesdatenschutzgesetzes beschlossen.[124] Damit sollen zum einen die (vermeintlichen) Spielräume, die die Grundverordnung dem nationalen Gesetzgeber durch die zahlreichen Öffnungsklauseln[125] lässt, genutzt werden. Zum anderen soll damit zu mehr Rechtssicherheit beigetragen werden. Der Entwurf wurde ähnlich kontrovers begleitet wie die Verordnung selbst, von verschiedenen Seiten teils heftig kritisiert und auch vielfach nachgebessert. Ob seine Regelungen vor dem Europäischen Gerichtshof bestehen können, bleibt aber abzuwarten. Die Europäische Kommission hat bereits im Entstehungsprozess des neuen Gesetzes mit einem Vertragsverletzungsverfahren gegen die Bundesrepublik Deutschland gedroht.[126] Viele der in der Verordnung verwendeten unbestimmte Rechtsbegriffe bedürfen einer Klärung durch den Europäischen Gerichtshof. Es wird daher vermutlich Jahre dauern, bis im Hinblick auf die Datenschutz-Grundverordnung Klarheit und Rechtssicherheit besteht.

„(…) Aufgrund der Unterkomplexität der Unionsregelungen sind mitgliedstaatliche Präzisierungen, Ausfüllungen und Ergänzungen notwendig, um die Verordnung problemadäquat und damit auf die faktischen Probleme, die es zu bewältigen gilt, anwendbar zu machen. In der Folge ist die Datenschutz-Grundverordnung kein homogenes, in sich geschlossenes Gesetzeswerk für den Datenschutz in der Union, sondern gleicht eher einem 'Schweizer Käse', der zwar einige strukturierende Elemente aufweist, vor allem aber durch die Löcher dazwischen auffällt. Anders als bei einem Schweizer Käse, werden diese Löcher aber unterschiedlich gefüllt werden. In der Folge wird kein einheitliches Datenschutzrecht in allen Mitgliedstaaten zur Anwendung kommen, sondern vergleichbar viele Unterschiede wie zuvor unter der Datenschutz-Richtlinie - nur an anderen Stellen und mit erheblicher Rechtsunsicherheit. (…)"[128]

(Prof. Dr. Alexander Roßnagel, Leiter des Fachgebiets Öffentliches Recht mit Schwerpunkt Recht der Technik und des Umweltschutzes)

129 Bitkom 2016.

130 Tripp 2015.

„Viele Regelungen der neuen Datenschutzverordnung sind so allgemein formuliert, dass nicht auf den ersten Blick klar ist, wie sie in der Praxis umgesetzt werden sollen. Das wird in der Anfangszeit zu einer gewissen Rechtsunsicherheit führen."[129]

(Susanne Dehmel, Mitglied der Geschäftsleitung Vertrauen und Sicherheit Bitkom e. V.)

„Das Projekt der Modernisierung des europäischen Datenschutzes ist aufgrund der Gegenwehr einiger Industriegruppen, die lieber im letzten Jahrhundert verharren wollen, leider nur teilweise geglückt. (...) Auch bedauern wir, dass es nicht gelungen ist, den schwammigen Begriff des 'berechtigten Interesses' für eine Datenverarbeitung zu reformieren. Wir sind jedoch froh, dass zumindest einige Schutzmaßnahmen ergänzt wurden. Schwerwiegender ist, dass das Vorhaben, den Datenschutz in der EU zu harmonisieren, in sein Gegenteil verkehrt wurde. Die Anzahl der Ausnahmetatbestände in der jetzigen Verordnung ist größer als die der eigentlichen Artikel in der bisher gültigen Richtlinie von 1995. (...)"[130]

(Gemeinsame Stellungnahme von European Digital Rights, Bits of Freedom, Digital Rights Ireland, Privacy International und Digitale Gesellschaft e. V.)

131 vzbv 2016.

132 Kemper 2016: S. 9.

133 Breyer 2015.

„Das Ja zur EU-Datenschutzverordnung ist eine gute Nachricht für Verbraucher und Unternehmen. Endlich gelten europaweit einheitliche und zeitgemäße Spielregeln beim Datenschutz."[131]

(Klaus Müller, Vorstand des Verbraucherzentrale Bundesverbands)

„Leider zeigt der verabschiedete Kompromiss zur Datenschutz-Grundverordnung mit aller Deutlichkeit, dass der europäische Gesetzgeber die Zeichen der Zeit nicht in allen Facetten erkannt hat. Sie stellt einen realitätsfernen, einwilligungsbasierten 'One size fits all'-Ansatz dar, der erhebliche Hürden für entgeltfreie Dienste, also den Kern des Internets, schafft."[132]

(Thomas Duhr, Vizepräsident Bundesverband Digitale Wirtschaft e. V.)

„Nach allem, was wir über den hinter verschlossenen Türen ausgehandelten und unter massivem Lobbyisteneinfluss geschlossenen Deal wissen, wird er nur in Einzelbereichen den Datenschutz stärken, in wichtigen Teilen aber das derzeitige Datenschutzniveau absenken: So wird das bisherige deutsche Verbot einer Protokollierung unseres Surfverhaltens im Netz durch Internet- und Medienkonzerne aufgegeben. Die offene Videoüberwachung von Büros soll weitreichend erlaubt werden – bisher war das in Deutschland nur in engen Grenzen als letztes Mittel zulässig. Außerdem soll gegen die Erstellung von Verbraucherprofilen nur ein Widerspruchsrecht bestehen."[133]

(Patrick Breyer, Piratenpartei, MdL Schleswig Holstein)

LITERATUR

Ackermann, Astrid (2016): Geändertes Gesetz: Datenschutz nun auch Verbraucherschutz, 24.06.2016, https://www.datenschutzbeauftragter-info.de/geaendertes-gesetz-datenschutz-nun-auch-verbraucherschutz/ [zuletzt geprüft am 15.02.2017].

Baker, Jennifer (2012): EU privacy watchdog expects no immediate change in data protection standoff with US, 05.12.2012, http://www.csoonline.com/article/2132628/privacy/eu-privacy-watchdog-expects-no-immediate-change-in-data-protection-standoff-with-us.html [zuletzt geprüft am 15.02.2017].

Baker, Jennifer (2013): Google, Microsoft, and Yahoo are secret backers behind European Privacy Association, infoworld, 20.5.2013, http://www.infoworld.com/article/2614554/startups/google--microsoft--and-yahoo-are-secret-Backers-behind-european-privacy-association.html [zuletzt geprüft am 15.02.2017].

Bergemann, Benjamin (2013): EU-Ministerrat reitet auf Trojanischen Pferden Richtung Datenschutzreform, netzpolitik.org, 11.03.2013, https://netzpolitik.org/2013/innen-und-justizminister-reiten-auf-trojanischen-pferden-richtung-datenschutzreform/ [zuletzt geprüft am 15.02.2017].

BEUC (o. J.): Privacy and personal data protection, http://www.beuc.eu/digital-rights/privacy-and-personal-data-protection [zuletzt geprüft am 27.04.2017].

Beuth, Patrick (2013): Alles Wichtige zum NSA-Skandal, Zeit online, 28.10.2013, http://www.zeit.de/digital/datenschutz/2013-10/hintergrund-nsa-skandal [zuletzt geprüft am 15.02.2017].

BfDI (2012): Die Europäischen Datenschutzbehörden verabschieden eine Stellungnahme zu den Reformvorschlägen zum Datenschutzrecht, 29.03.2012, https://www.bfdi.bund.de/DE/Europa_International/Europa/Reform_Datenschutzrecht/ReformEUDatenschutzrechtArtikel/Eu_Datenschutzbeh%C3%B6rden_verabsch_Stellungnahme_Reformvorschlaegen.html [zuletzt geprüft am 27.04.2017].

BfDI (o. J. a): Die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit, https://www.bfdi.bund.de/DE/BfDI/bfdi-node.html [zuletzt geprüft am 15.02.2017].

BfDI (o. J. b): Europäischer Datenschutz, http://www.bfdi.bund.de/DE/Europa_International/Europa/europa-node.html [zuletzt geprüft am 15.02.2017].

Biermann, Kai (2013): Mehr Datenschutz in der EU dank Snowden, Zeit online, 18.10.2013, http://www.zeit.de/digital/datenschutz/2013-10/eu-datenschutzreform-abstimmung-libe/komplettansicht [zuletzt geprüft am 15.02.2017].

Bitkom (2015): Big Data und europäisches Datenschutzrecht, 04.02.2015, https://www.bitkom.org/Lost-Found/20150204-Stellungnahme-Big-Data-und-Datenschutz.pdf [zuletzt geprüft am 27.04.2017].

Bitkom (2016): Datenschutzverordnung sollte einheitlich angewendet werden, Pressemitteilung, 14.04.2016, https://www.bitkom.org/Presse/Presseinformation/Datenschutzverordnung-sollte-einheitlich-angewendet-werden.html [zuletzt geprüft am 15.02.2017].

BMJV (2015): Effektive Durchsetzung von Verbraucherrechten: Verbandsklagerecht bei Datenschutzverstößen, 18.12.2015, https://www.bmjv.de/SharedDocs/Artikel/DE/2015/12182015_Verbandsklagerecht.html [zuletzt geprüft am 15.02.2017].

BMWi (2015): Monitoring-Report Wirtschaft DIGITAL 2015, https://www.bmwi.de/Redaktion/DE/Publikationen/Digitale-Welt/monitoring-report-wirtschaft-digital-2015.pdf?__blob=publicationFile&v=12 [zuletzt geprüft am 15.02.2017].

Breyer, Patrick (2015): Kommentar zu der Einigung auf ein EU-weit einheitliches Datenschutzrecht, Piratenpartei, MdL Schleswig Holstein, 17.12.2015, http://www.patrick-breyer.de/?p=560176 [zuletzt geprüft am 15.02.2017].

Bundesrat (2012): Subsidiaritätsrüge zur europäischen Datenschutz-Grundverordnung, Pressemitteilung, 30.03.2012; http://www.bundesrat.de/SharedDocs/pm/2012/051-2012.html [zuletzt geprüft am 15.02.2017].

Büschemann, Karl Heinz (2015): Große Datenfirmen könnten 'eine kleine Behörde lahmlegen', Süddeutsche Zeitung, 19.9.2015, http://www.sueddeutsche.de/digital/datenschutz-digitaler-sisyphos-1.2653568 [zuletzt geprüft am 15.02.2017].

BvD e. V. (2013): Optimistisch, dass es bis April 2014 eine Einigung gibt, BvD-News 2/2013, https://www.bvdnet.de/fileadmin/BvD_eV/pdf_und_bilder/Mitgliederbereich/Publikationen/BvD_News/z2013-02.pdf. [zuletzt geprüft am 15.02.2017].

BVDW e. V. (2013): Kommentar: EU-Datenschutz-Grundverordnung – Chance oder Risiko?, 18.10.2013, http://www.bvdw.org/medien/kommentar-eu-datenschutz-grundverordnung--chance-oder-risiko?media=5213 [zuletzt geprüft am 15.02.2017].

BVDW e. V. (2016): BVDW zur EU-Datenschutzreform: Überregulierung statt Rechtssicherheit, 15.04.2016, http://www.bvdw.org/medien/bvdw-zur-eu-datenschutzreform-berregulierung-statt-rechtssicherheit?media=7645 [zuletzt geprüft am 15.02.2017].

BVMW (2014): Positionspapier EU-Datenschutz-Grundverordnung, 20.12.2014, https://www.bvmw.de/fileadmin/download/Downloads_allg._Dokumente/politik/positionspapiere/positionspapier_eu-datenschutz-grundverordnung.pdf [zuletzt geprüft am 15.02.2017].

Center for Democracy & Technology (o. J.): Privacy & Data, https://cdt.org/issue/privacy-data/ [zuletzt geprüft am 15.02.2017].

Clarke, Adele (2005): Situational Analysis. Grounded Theory after the Postmodern Turn, Thousand Oaks, California: Sage.

Datenschutzbeauftragter INFO (2014): Datenschutzbeauftragte von Bund und Ländern, 27.05.2014, https://www.datenschutzbeauftragter-info.de/datenschutzbeauftragte-von-bund-und-laendern/ [zuletzt geprüft am 15.02.2017].

De Maizière, Thomas (2016): Deutschland bleibt ein sicheres Land, Pressekonferenz zu geplanten Maßnahmen zur Erhöhung der Sicherheit in Deutschland, 11.08.2016, http://www.bmi.bund.de/SharedDocs/Kurzmeldungen/DE/2016/08/pressekonferenz-zu-massnahmen-zur-erhoehung-der-sicherheit-in-deutschland.html;jsessionid=19B88F99A3593058F768AE4FBDE8D9CF.2_cid364?nn=3314802 [zuletzt geprüft am 15.02.2017].

Dehmel, Susanne (2015): Nachbesserungen bei EU-Datenschutzverordnung notwendig, Pressemitteilung, 15.06.2015, https://www.bitkom.org/Presse/Presseinformation/Nachbesserungen-bei-EU-Datenschutzverordnung-notwendig.html [zuletzt geprüft am 15.02.2017].

Die Welt (2013): Merkel will internationales Datenschutzabkommen, 14.07.2013, https://www.welt.de/newsticker/dpa_nt/infoline_nt/brennpunkte_nt/article118035131/Merkel-will- internationales-Datenschutzabkommen.html [zuletzt geprüft am 15.02.2017].

Digitalcourage (o. J.): Über uns, https://digitalcourage.de/ueber-uns [zuletzt geprüft am 27.04.2017].

Digitale Gesellschaft e. V. (2013): Internationale Bürgerrechtsorganisationen: Unternehmen gefährden unsere Grundrechte auf Privatsphäre und Datenschutz, 25.04.2013, https://digitalegesellschaft.de/wp-content/uploads/2013/04/EUDATAP_REPORT_DE1-0.pdf [zuletzt geprüft am 15.02.2017].

DigitalEurope (2014): Making Europe Fit for the Data Economy, 09.12.2014, http://www.digitaleurope.org/DesktopModules/Bring2mind/DMX/Download.aspx?Command=Core_Download&EntryId=864&language=en-US&PortalId=0&TabId=353 [zuletzt geprüft am 15.02.2017].
DigitalEurope (2015): Pressemitteilung, 15.06.2015, http://www.digitaleurope.org/DesktopModules/Bring2mind/DMX/Download.aspx?Command=Core_Download&EntryId=979&language=en-US&PortalId=0&TabId=353 [zuletzt geprüft am 15.02.2017].
Ebbinghaus, Uwe/Schulz, Stefan/Thiel, Thomas (2014): Machtprobe mit Silicon Valley, FAZ, 11.03.2014, http://www.faz.net/aktuell/feuilleton/debatten/die-digital-debatte/europas-it-projekt/digitale-agenda- machtprobe-mit-silicon-valley-12842407.html [zuletzt geprüft am 15.02.2017].
EDRi (2012): EDRi Initial Comments on the Proposal for a Data Protection Regulation, 27.01.2012, https://edri.org/commentsdpr/ [zuletzt geprüft am 15.02.2017].
EDRi (2013): Protecting privacy while maintaining global trade and security requires flexible solutions, https://edri.org/files/us_position_20130114.pdf [zuletzt geprüft am 15.02.2017].
EDRi (o. J.): Why we do it, https://edri.org/why-we-do-it/ [zuletzt geprüft am 27.04.2017].
Europäische Kommission (2012): Kommission schlägt umfassende Reform des Datenschutzrechts vor, um Nutzern mehr Kontrolle über ihre Daten zu geben und die Kosten für Unternehmen zu verringern, Pressemitteilung, 25.2.2012, http://europa.eu/rapid/press-release_IP-12-46_de.htm [zuletzt geprüft am 15.02.2017].
Europäische Kommission (2013): Commission welcomes European Parliament rapporteurs´ support for strong EU data protection rules, 10.01.2013, http://europa.eu/rapid/press-release_MEMO-13-4_de.htm [zuletzt geprüft am 15.02.2017].
Europäische Union (o. J., a): Die EU - kurz gefasst, https://europa.eu/european-union/about-eu/eu-in-brief_de [zuletzt geprüft am 15.02.2017].
Europäische Union (o. J., b): Gerichtshof der Europäischen Union (EuGH), https://europa.eu/european-union/about-eu/institutions-bodies/court-justice_de [zuletzt geprüft am 15.02.2017].
Europäisches Parlament (2014): Parlament verschärft Regeln zum Schutz persönlicher Daten im digitalen Zeitalter, Plenartagung Pressemitteilung, 12.03.2014, http://www.europarl.europa.eu/news/de/news-room/20140307IPR38204/parlament-versch%C3%A4rft- regeln-zum-schutz-pers%C3%B6nlicher-daten-im-digitalen-zeitalter [zuletzt geprüft am 15.02.2017].
European Privacy Association (o. J.): Mission, http://europeanprivacyassociation.eu/mission/ [zuletzt geprüft am 15.02.2017].
Fox, Benjamin (2012): Police should not be exempt from privacy rules, says EU data chief, EUobserver, 21.6.2012, https://euobserver.com/justice/116706 [zuletzt geprüft am 15.02.2017].
Fox, Benjamin (2013): EU commission ´stood firm´ on US data privacy, EUobserver, 13.06.2013, https://euobserver.com/justice/120490 [zuletzt geprüft am 15.02.2017].
Geminn, Christian L. (2015): Crypto Wars Reloaded?. In: DuD - Datenschutz und Datensicherheit 39 (8), S. 546 – 547.
Geminn, Christian L. (2016): Demokratie zwischen Öffentlichkeit und Privatheit. In: VerwArch - Verwaltungsarchiv 107 (4), S. 601 – 630.
Hogan Lovells (2012a): US Government Tells EU: „We Are Adequate", 06.12.2012, https://www.hoganlovells.com/en/blogs/hldataprotection/us-government-tells-eu-we-are-adequate [zuletzt geprüft am 15.02.2017].
Hogan Lovells (2012b): Forum Europe's 3rd Annual European Data Protection and Privacy Conference, 04.12.2012, https://www.hoganlovells.com/en/blogs/hldataprotection/us-government-tells-eu-we-are-adequate [zuletzt geprüft am 15.02.2017].
Industry coalition for data protection (2012): Reforming Europe´s Privacy Framework - How to find the right balance, September 2012, http://www.digitaleurope.org/DocumentDownload.aspx?Command=Core_Download&EntryId=545 [zuletzt geprüft am 15.02.2017].
Initiative Data Protection in Europe (2013): Positionspapier zur Datenschutz-Grundverordnung, http://web.archive.org/web/20160304212653/http://dataprotectioneu.eu/index_de.html. [zuletzt geprüft am 15.02.2017].
Kemper, Frank (2016): INTERNET WORLD Business 2/2016, S. 8 – 10, http://heftarchiv.internetworld.de/content/download/123047/3378157/file/IWB_0216_Klein.pdf [zuletzt geprüft am 15.02.2017].
Klein, Matthias (2014): Ist die Europäische Union demokratisch genug?, bpb, 07.04.2014, https://www.bpb.de/dialog/europawahl-blog-2014/181851/ist-die-europaeische-union-demokratisch -genug [zuletzt geprüft am 15.02.2017].
Konferenz der Datenschutzbeauftragten des Bundes und der Länder (2015): Datenschutzrechtliche Kernpunkte für die Trilogverhandlungen der Datenschutz-Grundverordnung, 14.08.2015, http://www.bfdi.bund.de/SharedDocs/Publikationen/Entschliessungssammlung/DSBundLaender/20150826_Verbesserung%20DSGrundverordnung.pdf?__blob=publicationFile&v=3 [zuletzt geprüft am 15.02.2017].
Krempl, Stefan (2013): EU-Parlament gibt grünes Licht für Datenschutzreform, heise online, 21.10.2013, http://www.heise.de/newsticker/meldung/EU-Parlament-gibt-gruenes-Licht-fuer-Datenschutzreform-1983124.html [zuletzt geprüft am 15.02.2017].
Krempl, Stefan (2017), Datenschutzreform: EU-Kommission droht Deutschland mit Vertragsverletzungsverfahren, heise online, 20.04.2017, https://www.google.com/url?q=https://www.heise.de/newsticker/meldung/Datenschutzreform-EU-Kommission-droht-Deutschland-mit-Vertragsverletzungsverfahren-3689759.html?wt_mc%3Dnl.ho.2017-04-21&sa=D&ust=1493392609439000&usg=AFQjCNHAsbqYSP-VaLvDU8F_mn_QX35EiA [zuletzt geprüft am 27.04.2017].
Lischka, Konrad/Stöcker, Christian (2013): Website entlarvt Lobby-Einfluss in Brüssel, Spiegel Online, 11.02.2013, http://www.spiegel.de/netzwelt/netzpolitik/lobbyplag-zeigt-lobby-einflussname-bei-eu-datenschutz-richtlinie-a-882567.html [zuletzt geprüft am 15.02.2017].
Lobbyplag (o. J. a), http://lobbyplag.eu/governments [zuletzt geprüft am 01.12.2016]
Lobbyplag (o. J. b), http://lobbyplag.eu/governments/documents [zuletzt geprüft am 01.12.2016]
Masing, Johannes (2012): Ein Abschied von den Grundrechten, Süddeutsche Zeitung, 09.01.2012, https://www.datenschutzbeauftragter-online.de/wp-content/uploads/2012/01/20120109_SZ_Masing_Datenschutz.pdf [zuletzt geprüft am 15.02.2017].
Menz, Michael (2016): Schriftliche Stellungnahme zum öffentlichen Fachgespräch zur Datenschutz-Grundverordnung am 24. Februar 2016 im Ausschuss Digitale Agenda des Deutschen Bundestags, Zalando SE, A-Drs. 18 (24) 97, 13.04.2016, https://www.bundestag.de/blob/418118/64f73092f5748d9cbe29a02832c2fae9/stellungnahme_menz-data.pdf. [zuletzt geprüft am 15.02.2017].
Merkel, Angela (2013): ARD-Sommerinterview, 14.07.2013, http://www.ardmediathek.de/tv/Bericht-aus-Berlin/Bericht-aus-Berlin-Sommerinterview-mit/Das-Erste/Video?bcastId=340982&-

documentId=15861418https://www.welt.de/newsticker/dpa_nt/infoline_nt/brennpunkte_nt/article118035131/Merkel-will-internationales-Datenschutzabkommen.html [zuletzt geprüft am 01.12.2016].
Merkel, Angela (2015): Rede von Bundeskanzlerin Merkel beim 9. Nationalen IT-Gipfel, 19.11.2015, https://www.bundesregierung.de/Content/DE/Rede/2015/11/2015-11-19-merkel-it-gipfel.html [zuletzt geprüft am 15.02.2017].
Müller, Klaus (2015): EU-Datenschutzverordnung: Verbraucherrechte müssen im Trilog geschärft werden, Pressemitteilung, 16.06.2015, http://www.vzbv.de/pressemitteilung/eu-datenschutzverordnung-verbraucherrechte-muessen-im-trilog-Geschaerft-werden [zuletzt geprüft am 15.02.2017].
Nielsen, Nikolaj (2012): Commission data protection reforms under fire, EUobserver, 03.05.2012, https://euobserver.com/justice/116129 [zuletzt geprüft am 15.02.2017]
Nielsen, Nikolaj (2013a): EU countries back pro-business data bill, EUobserver, 06.06.2013, https://euobserver.com/justice/120407 [zuletzt geprüft am 15.02.2017].
Nielsen, Nikolaj (2013b): EU data bill exposes political rifts, EUobserver, 15.05.2013, https://euobserver.com/news/120134 [zuletzt geprüft am 15.02.2017].
Nielsen, Nikolaj (2015a): EU ministers back weaker data protection rules, EUobserver, 15.06.2015, https://euobserver.com/justice/129122 [zuletzt geprüft am 15.02.2017].
Nielsen, Nikolaj (2015b): National governments punch holes in EU data protection bill, EUobserver, 03.03.2015, https://euobserver.com/justice/127856 [zuletzt geprüft am 15.02.2017].
n-tv (2014): Oettinger macht Digitales zu seinem Thema, 29.09.2014, http://www.n-tv.de/politik/Oettinger-macht-Digitales-zu-seinem-Thema-article13696331.html [zuletzt geprüft am 15.02.2017].
O´Brien, Kevin J. (2013): Silicon Valley Companies Lobbying Against Europe´s Privacy Proposals, The New York Times, 25.01.2013, http://www.nytimes.com/2013/01/26/technology/eu-privacy-proposal-lays-bare-differences-with-us.html?_r=1& [zuletzt geprüft am 15.02.2017].
Oetjen, Jan (2016): Schriftliche Stellungnahme zum öffentlichen Fachgespräch zur Datenschutz-Grundverordnung am 24. Februar 2016 im Ausschuss Digitale Agenda des Deutschen Bundestags, United Internet, A-Drs. 18 (24) 97, 19.02.2016, https://www.bundestag.de/blob/409388/4813873f2e4d425b3b16cc35bac0c297/a-drs-18-24-91-data.pdf [zuletzt geprüft am 15.02.2017].
Ombudsman Europa (2016): Ombudsman O'Reilly, Emiliy calls for more trilogues transparency, Pressemitteilung, 14.07.2016, https://www.ombudsman.europa.eu/press/release.faces/en/69214/html.bookmark [zuletzt geprüft am 15.02.2017].
Peters, Roland (2013): EU-Verordnung per "Copy & Paste" - Blog deckt Lobbyeinfluss auf, n-tv, 12.02.2013, http://www.n-tv.de/politik/Blog-deckt-Lobbyeinfluss-auf-article10103291.html [zuletzt geprüft am 15.02.2017].
Pop, Valentina (2013): Facebook, Skype challenged in EU over spy affair, EUobserver, 18.07.2013, https://euobserver.com/justice/120894 [zuletzt geprüft am 15.02.2017].
Privacy international (o. J.): No one shall be subjected to arbitrary interference with his privacy, family, home, or correspondence, https://www.privacyinternational.org/ [zuletzt geprüft am 27.04.2017].
Rat der Europäischen Union (2013): 3228th Council meeting Justice and Home Affairs, Pressemitteilung, 07./ 08. 03.2013, https://www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/en/jha/135901.pdf [zuletzt geprüft am 15.02.2017].

Rat der Europäischen Union (2015): Datenschutz: Rat legt allgemeine Ausrichtung fest, Pressemitteilung, 15.06.2015, http://www.consilium.europa.eu/de/press/press-releases/2015/06/15-jha-data-protection/ [zuletzt geprüft am 15.02.2017].
Richter, Philipp (2015): Datenschutz zwecklos? – Das Prinzip der Zweckbindung im Ratsentwurf der DSGVO. In: DuD - Datenschutz und Datensicherheit 39 (11), S. 735 – 740.
Roßnagel, Alexander (2016): Schriftliche Stellungnahme zum öffentlichen Fachgespräch zur Datenschutz-Grundverordnung am 24. Februar 2016 im Ausschuss Digitale Agenda des Deutschen Bundestags, A-Drs. 18 (24) 94, 19.02.2016, https://www.bundestag.de/blob/409512/4afc3a566097171a7902374da77cc7ad/a-drs-18-24-94-data.pdf [zuletzt geprüft am 15.02.2017].
Roßnagel, Alexander (Hg.) (2017): Europäische Datenschutz-Grundverordnung. Vorrang des Unionsrechts - Anwendbarkeit des nationalen Rechts, 1. Auflage, Baden-Baden: Nomos.
Roßnagel, Alexander/Kroschwald, Steffen (2014): Was wird aus der Datenschutzgrundverordnung? - Die Entschließung des Europäischen Parlaments über ein Verhandlungsdokument. In: Zeitschrift für Datenschutz Heft 10/2014, S. 495 – 500.
Roßnagel, Alexander/Nebel, Maxi/Richter, Philipp (2015): Was bleibt vom Europäischen Datenschutzrecht? Überlegungen zum Ratsentwurf der DS-GVO. In: Zeitschrift für Datenschutz Heft 10/2015, S. 455 – 460.
Schmiechen, Frank (2015): Das Internet hat uns gehört, Gründerszene, 16.02.2015, http://www.gruenderszene.de/allgemein/obama-recode-interview [zuletzt geprüft am 15.02.2017].
Strauss, Anselm L. (1978): A Social World Perspective. In: Studies in Symbolic Interaction, Band 1, S. 119 – 128.
Strauss, Anselm L. (1993): Continual Permutations of Action. Hawthorne, New York: de Gruyter.
Stupp, Catherine (2015): EU watchdog launches transparency app for data privacy talks, euractiv, 27.7.2015, https://www.euractiv.com/section/digital/news/eu-watchdog-launches-transparency-app-for-data-privacy-talks/ [zuletzt geprüft am 15.02.2017].
Tripp, Volker (2015): Vorentscheidung zur Europäischen Datenschutzgrundverordnung: am Ende reichte es nur zur Sicherung von Mindeststandarts, Digitale Gesellschaft, 17.12.15, https://digitalegesellschaft.de/2015/12/vorentscheidung-dsgvo-mindeststandard/ [zuletzt geprüft am 15.02.2017].
Tzschentke, Karin (2013): Massives Lobbying gegen EU-Datenschutzverordnung, Der Standard, 13.02.2013, http://derstandard.at/1360161300194/Massives-Lobbying-gegen-Datenschutzverordnung [zuletzt geprüft am 15.02.2017].
Verein Für soziales Leben e. V. (o. J.): Welche Regelungen beinhaltet die Europäische Datenschutz-Grundverordnung - DSGVO-EU?, http://www.europaeische-datenschutz-grundverordnung.de/inhalt.html [zuletzt geprüft am 15.02.2017].
vzbv e. V. (2012): Datenschutz-Grundverordnung: Gute Ideen, aber zu vage, Stellungnahme, 29.02.2012, http://www.vzbv.de/dokument/datenschutz-Grundverordnung-gute-ideen-aber-zu-vage [zuletzt geprüft am 15.02.2017].
vzbv e. V. (2016): Besserer Datenschutz für Verbraucher, Pressemitteilung, 14.04.2016, http://www.vzbv.de/pressemitteilung/besserer-datenschutz-fuer-verbraucher [zuletzt geprüft am 15.02.2017].
vzbv e. V. (o. J.): EU-Datenschutzverordnung, http://www.vzbv.de/eu-datenschutzverordnung [zuletzt geprüft am 27.04.2017].
Warren, Samuel D./Brandeis, Louis D. (2012 [1890]): Das Recht auf Privatheit – The Right to Privacy. Harv. L. Rev. 4/1890, 193, übersetzter Nachdruck, In: DuD - Datenschutz und Datensicherheit 36 (10): S. 755 – 766.

BMBF-Projekt “Kartographie und Analyse der Privacy-Arena”

Januar 2014 bis Dezember 2016

Privatheit ist zu einem umstrittenen und unsicheren Begriff geworden. Das BMBF-Projekt "Kartografie und Analyse der Privacy-Arena" untersuchte deshalb die politischen Prozesse, die diesen Wandel von Privatheit vorantreiben, begrenzen und bewerten. Exemplarisch untersucht wurden dafür öffentliche Auseinandersetzungen rund um Privatheit. Diese Debatten und Streitfälle versammeln auf je unterschiedliche Weisen wichtige Instanzen und Akteurinnen einer Neuverhandlung des Privaten. Die verschiedenen Situationen können deshalb verstanden werden als relevante Ausschnitte der Privacy-Arena, in der koalierend und konfligierend die Zukunft des Privaten und die Verfasstheit der digitalen Welt verhandelt werden. Das Projekt will durch diese beispielhaften Erkundungen unterschiedliche demokratische Reaktions- und Artikulationsweisen und die damit einhergehenden Zugriffsweisen auf Privatheit empirisch erfassen und zueinander in Verhältnis setzen. Das Verbundprojekt, bestehend aus den Disziplinen Soziologie, Rechtswissenschaft und Ethik, kooperierte seit Herbst 2015 mit einer Gruppe des Studiengangs Visuelle Kommunikation der Kunsthochschule Kassel. Im Rahmen dieser Zusammenarbeit wurden Visualisierungen der wissenschaftlichen Projektergebnisse erarbeitet.

Projektleitung
Prof. Dr. Jörn Lamla
Fachgebiet Soziologische Theorie,
Universität Kassel

Dr. Carsten Ochs
Fachgebiet Soziologische Theorie
Universität Kassel

Mitarbeiter*innen
Barbara Büttner
Fabian Pittroff

Hilfskräfte
Enrico Hörster
Annika Schmitt

Projektpartner*innen
Prof. Dr. Regina Ammicht Quinn
Internationales Zentrum für Ethik in den Wissenschaften
Universität Tübingen

PD Dr. Jessica Heesen
Internationales Zentrum für Ethik in den Wissenschaften
Universität Tübingen

Mitarbeiter*innen
Andreas Baur-Ahrens
Dr. Thilo Hagendorff
Maria Pawelec

Prof. Dr. Alexander Roßnagel
Leiter des Fachgebiets Öffentliches Recht
Universität Kassel

Mitarbeiter*innen
Charlotte Barlag
Dr. Christian Geminn
Nadine Miedzianowski

Künstler*innen
Prof. Joel Baumann
Rektor/Professur für Neue Medien,
Kunsthochschule Kassel

Jörn Röder
Künstlerischer Mitarbeiter Neue Medien
Visuelle Kommunikation

Mike Huntemann
Student Neue Medien
Visuelle Kommunikation

Isabel Paehr
Studentin Neue Medien
Visuelle Kommunikation

DANKE

Herzlich danken möchten wir den Künstler*innen, den Projektpartner*innen sowie den Mitarbeiter*innen, den Gestalter*innen, den studentischen Hilfskräften, den Studierenden des Empiriepraktikums „Kontroversen kartografieren“ und allen anderen Unterstützer*innen sowie dem BMBF als Förderer dieses Projekts.

Joel Baumann, Jörn Lamla


BRD
USA
Irland
Antibundnahmen

IMPRESSUM

HERAUSGEBER:
Joel Baumann, Jörn Lamla

AUTOR*INNEN:
Charlotte Barlag, Joel Baumann, Andreas Baur-Ahrens, Barbara Büttner, Christian Geminn, Thilo Hagendorff, Mike Huntemann, Jörn Lamla, Nadine Miedzianowski, Isabel Paehr, Maria Pawelec, Fabian Pittroff, Jörn Röder

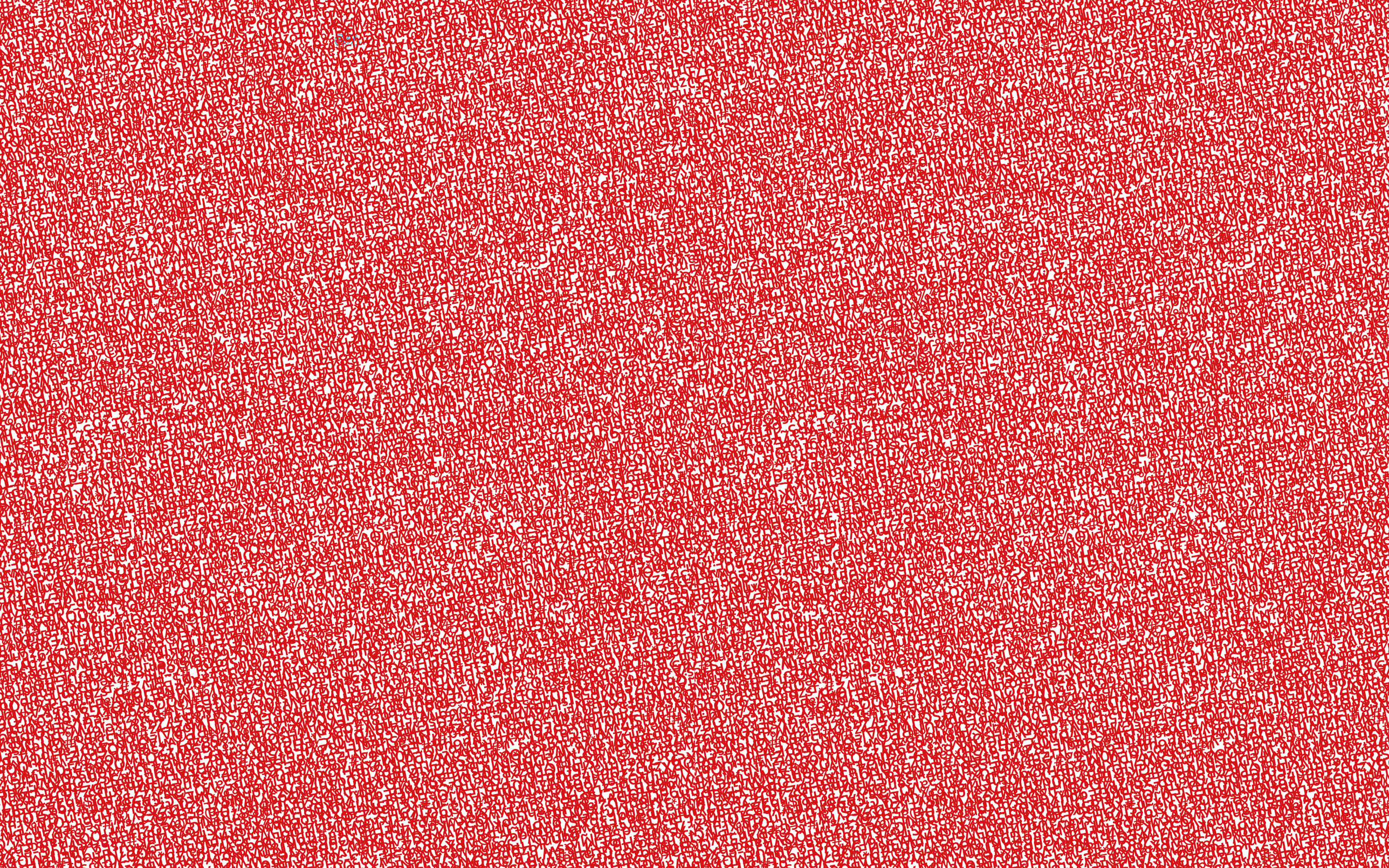
LAYOUT:
Jörn Röder, Britta Wagemann

FOTOS:
Holger Jenss

GRAFIKEN:
Mike Huntemann, Isabel Paehr, Jörn Röder

Bibliografische Information der Deutschen Nationalbibliothek
Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über http://dnb.dnb.de abrufbar

ISBN: 978-3-7376-0306-5 (print)
ISBN: 978-3-7376-0307-2 (e-book)
DOI: http://dx.medra.org/10.19211/KUP9783737603072
URN: http://nbn-resolving.de/urn:nbn:de:0002-403074



PRI-VACY ARENA

Kontroversen um Privatheit im digitalen Zeitalter

Privatheit ist in Zeiten von Digitalisierung und Vernetzung umstritten und umkämpft. Nicht nur für Staaten entstehen neue Überwachungsmöglichkeiten, auch für Unternehmen eröffnen sich Geschäftsmodelle, die klassische Vorstellungen von Privatheit in Frage stellen.

In dieser Situation der Neuorientierung hilft es, von Definitionsversuchen abzusehen und stattdessen in die vielen Kontroversen um die Zukunft der Privatheit einzutauchen. Diesen Ansatz verfolgt das BMBF-Forschungsprojekt „Kartografie und Analyse der Privacy-Arena". In Zusammenarbeit der Disziplinen Soziologie, Rechtswissenschaft, Ethik und Visuelle Kommunikation wurden politische Kämpfe um die Bedeutung und den ethischen und rechtlichen Stellenwert von Privatheit wissenschaftlich und künstlerisch aufgearbeitet. Zu den konkret untersuchten Kontroversen gehören die politischen Momente von Technologien wie Kryptografie, die demokratischen Strategien gegenüber staatlicher Überwachung im NSA-Untersuchungsausschuss des Bundestages, die unübersichtlichen Folgen der algorithmischen Realitätserzeugung durch Big Data und die widerstreitenden Interessen hinsichtlich der Einführung einer europäischen Datenschutz-Grundverordnung. Das Vorgehen des Forschungsvorhabens folgt Ansätzen der Science and Technology Studies, der Akteur-Netzwerk-Theorie, den Mapping-Verfahren der Situationsanalyse von Adele Clarke und der Theorie sozialer Welten und Arenen von Anselm Strauss. Ergänzt wurde bzw. wird dieser Band durch eine im Dezember 2016 in Kassel stattgefundene Ausstellung sowie der Homepage **privacy-arena.net.**

MIT BEITRÄGEN VON:
Andreas Baur-Ahrens, Charlotte Barlag, Joel Baumann, Barbara Büttner, Christian Geminn, Thilo Hagendorff, Mike Huntemann, Jörn Lamla, Nadine Miedzianowski, Isabel Paehr, Maria Pawelec, Fabian Pittroff, Jörn Röder

HERAUSGEGEBEN VON:
Joel Baumann, Jörn Lamla

ISBN: 978-3-7376-0306-5

PARTNER*INNEN UND UNTERSTÜTZER*INNEN

forum <privatheit>
Selbstbestimmtes Leben in der digitalen Welt

GEFÖRDERT VOM
Bundesministerium für Bildung und Forschung