Privacy-Arena

Analyse und Kartografie der Privacy-Arena

Schlussbericht

FKZ 16KIS0097

Laufzeit: 1. November 2013 bis 31. Dezember 2016

Projektleitung:

Prof. Dr. Regina Ammicht Quinn

PD Dr. Jessica Heesen

Internationales Zentrum für Ethik in den Wissenschaften (IZEW)
Eberhard Karls Universität Tübingen
Telefon: 07071 29-77983
E-Mail: regina.ammicht-quinn@uni-tuebingen.de, jessica.heesen@uni-tuebingen.de

Projektteam:

Andreas Baur-Ahrens (2015–2016)

Dr. Thilo Hagendorff (2013–2016)

Jutta Krautter (2013–2014)

Simon Ledder (2014–2015)

Maria Pawelec (2016)

Tübingen, 28.06.2017

EBERHARD KARLS UNIVERSITÄT TÜBINGEN

Internationales Zentrum für Ethik in den Wissenschaften (IZEW)

Inhalt

1 Kurze Darstellung

1.1 Aufgabenstellung

Gegenwärtig gibt es, ausgelöst durch ein breites gesellschaftliches Problembewusstsein, zahlreiche politische Auseinandersetzungen, in denen Fragen nach dem ethischen und rechtlichen Stellenwert von Privatheit verhandelt werden. Dies ist insbesondere der Verbreitung informationstechnischer Systeme geschuldet. Im Kontext dieser Systeme kann Privatheit definiert werden über die Kontrolle, die eine Person darüber ausübt, wer Zugriff auf persönlichkeitsrelevante Daten und Informationen hat. Die Frage ist aber, wie weit diese Kontrolle überhaupt noch reicht, bedenkt man etwa die datenschutzrechtlich fraglichen Praktiken von Google, Facebook und ähnlichen Diensten. Je mehr persönlichkeitsrelevante Informationen zur elektronisch tauschbaren, wirtschaftlich verwertbaren Ressource werden, desto mehr werden etablierte Beschränkungen zur Verbreitung und Weitergabe von Informationen aufgelöst. Für Wirtschaftsunternehmen sind gerade personenbezogene Daten von großem Wert, schließlich erlaubt der Besitz dieser Daten, dass zielgenaue Kaufanreize beispielsweise über personalisierte Onlinewerbung gesetzt werden können. Aus dem Zusammenspiel wirtschaftlicher, polizeilicher, geheimdienstlicher, staatlicher wie auch persönlicher Interessen an personenbezogenen Daten sowie den Möglichkeiten informationstechnischer Systeme entsteht eine Dynamik, welche einerseits die Auflösung eines etablierten Verständnisses von Privatsphäre vorantreibt, aber andererseits neue Begriffe des Privaten sowie vielfältige Praxen der Grenzziehung zwischen Privatheit und Öffentlichkeit hervorbringt.

Die Forschung fokussierte sich auf die Kartografie und Analyse der Privacy-Arena. Hierbei ging es darum, den normativen Stellenwert der Privatheit aus den Konfliktzonen und Diskursen, welche in der Arena geführt werden, empirisch zu rekonstruieren und hermeneutisch zu analysieren. Die Privacy-Arena steht dabei „pars pro toto“ für die Kontroversen um eine Ordnung der digitalen Gesellschaft. Ein Schwerpunkt lag dabei auf den Themenfeldern Big Data und (Gegen-)Überwachung. Das Forschungsprojekt zielte auf eine normative Analyse der Konfliktzonen, welche sich zwischen der Privatsphäre, deren Verflechtung mit informationstechnischen Systemen sowie den Regulierungsinteressen der Politik aufspannen. Die fortschreitende Nutzung von Informationstechniken in sämtlichen Gesellschaftsbereichen legt nahe, dass eine zunehmende Entgrenzung zwischen Privatheit und Öffentlichkeit stattfindet und dass sich überkommene normative Ordnungen des Privaten im Wandel befinden. Entsprechend bestand ein Forschungsziel des Projekts in der Bestimmung des theoretischen Status von Privatheit unter aktuellen technologischen und sozialen Bedingungen. Dabei wurde untersucht, inwiefern eine demokratisch organisierte, politische Steuerung dieses Wandels möglich und wünschenswert ist. Gemeinsam mit den Projektpartnern aus Soziologie und Recht der Universität Kassel wurden ethische, lebenspraktische sowie rechtliche Grauzonen freigelegt, die aus der Neuordnung der für die Privatsphäre konstitutiven Normen resultieren. Darüber hinaus war es ein wichtiges Ziel, die Ergebnisse des Projekts in gut verständlicher, visuell aufbereiteter Form für interessierte Bürgerinnen und Bürger zur Verfügung zu stellen.

1.2 Voraussetzungen, unter denen das Vorhaben durchgeführt wurde

Das Projekt Privacy-Arena war ein wissenschaftliches Verbundprojekt, welches u.a. am Internationalen Zentrum für Ethik in den Wissenschaften (IZEW) der Universität Tübingen

unter Leitung von Prof. Dr. Regina Ammicht Quinn und PD Dr. Jessica Heesen durchgeführt wurde. Die Arbeitspakete wurden von Jutta Krautter (von 2013 bis 2014), Simon Ledder (von 2014 bis 2015), Andreas Baur-Ahrens (ab 2015), Maria Pawelec (ab 2016) und Dr. Thilo Hagendorff (ab 2013) bearbeitet.

1.3 Planung und Ablauf des Vorhabens

Das Projekt gliederte sich in die Phase 1 des Erstantrags und die Phase 2 des Verlängerungsantrags.

Phase 1 (1.11.2013 bis 31.12.2014)

AP 1: Identifizierung eines exemplarischen Segments der Arena

AP 2: Grundlegende Fragen

AP 3: Reflexion der empirischen Untersuchungen zur Privacy-Arena

AP 4 Zusammenführung und Verdichtung von Hypothesen zur Privacy-Arena und ihrer gesellschaftlichen Entwicklung

Phase 2 (01.01.2015 bis 31.12.2016)

AP 1: Privatheit und Demokratie

AP 2: Analyse der vier weiteren Arena-Segmente

AP 3: Dekontextualisierung und Kontrolle von Information

AP 4: Visuelle Kommunikation

AP 5: Methodenreflexion

AP 6: Zusammenführung der Ergebnisse

AP 7: Publikation

1.4 Wissenschaftlicher und technischer Stand, an den angeknüpft wurde

Das Projekt Privacy-Arena hat an den Forschungs- und Wissenstand in den folgenden Feldern angeknüpft (für Details siehe die Ausführungen im ausführlichen Bericht über die Arbeitspakete):

- Stand der Forschung im Themenbereich Privatheit: Indem in regelmäßigen Abständen einschlägige Fachzeitschriften durchgesehen wurden, wurden die Publikationen, welche zum Thema Privatheit erscheinen, erfasst und in der eigenen Forschung verwendet.
- Stand der Technik im Bereich digitaler Medien: Hier wurde über Tagungsbesuche, Nachricht und Fachzeitschriften die Entwicklung im Bereich digitaler Medien nachgehalten. Ohne detaillierte Kenntnisse über technische Aspekte des Medienwandels in der digitalen Gesellschaft wäre die Forschung zur Privacy-Arena nicht möglich gewesen.

Der Stand der Forschung wurde über den gesamten Projektverlauf anhand von Literatur- und Internetrecherchen sowie durch Konferenz- und Tagungsbesuche fortgeschrieben. Es wurde eine Literaturdatenbank in der Literaturverwaltungssoftware Citavi angelegt, die fortlaufend aktualisiert wurde.

1.5 Angabe der verwendeten Fachliteratur

Es wurde durch Literatur- und Journalrecherchen möglichst umfassend die wichtigsten Publikationen, welche für die Forschung zu Privatheit relevant sind, recherchiert, in eine Literaturdatenbank eingespeist und für die eigene Forschung benutzt.

1.6 Zusammenarbeit mit anderen Stellen

Das Verbundprojekt fand in Zusammenarbeit statt mit dem Fachbereich Soziologie (Prof. Dr. Jörn Lamla, Leitung des Verbundprojekts), dem Fachbereich Öffentliches Recht der Universität Kassel (Prof. Dr. Alexander Roßnagel), sowie der Professur für Neue Medien, Kunsthochschule Kassel (Prof. Joel Baumann).

2 Eingehende Darstellung

2.1 Erzielte Ergebnisse

2.1.1 Arbeitspakete des Erstantrags

AP 1: Identifizierung eines exemplarischen Segments der Arena, in dem sich charakteristische Privacy-Probleme manifestieren

Ziele: Festlegung auf ein zu erforschendes Arena-Segment sowie Identifizierung der daran beteiligten Welten.

Arbeitsschritte und erzielte Ergebnisse:

- Im Rahmen des ersten Arbeitspaketes ging es um die Identifizierung eines exemplarischen Segments der Privacy-Arena, in welcher sich charakteristische Privatheits-Probleme manifestieren. Hier fiel die Wahl auf die Bemühungen um die Etablierung nationaler Routingprogramme. Verschiedene Akteure vor allem aus Wirtschaft und Politik sprachen sich für die Einführung nationaler Routingprogramme aus. Diese erstrecken sich entweder auf die Bundesrepublik Deutschland („Schland-Netz“) oder die Schengen-Staaten („Schengennetz“). Nationale Routingprogramme sind als eine Reaktion auf die globale Überwachungs- und Spionageaffäre, welche durch die Enthüllungen des Whistleblowers Edward Snowden ausgelöst wurde, zu betrachten. Unter dem Arbeitstitel „Reterritorialisierung des Netzes“ wurden die Verhandlungen zu einer Einhegung des Internets im Rahmen nationaler Routingprogramme untersucht.
- Die Akteur_innen, die an den Konflikten um ein Schengen-Routing beteiligt waren, wurden in einer breiten Analyse erfasst. Zudem fand eine ethische Aufarbeitung des Problemgehalts des Schengen-Routings statt. Dabei wurde die Rolle von Vertrauen bzw. Systemvertrauen im Kontext des Routings bzw. der Internetkommunikation in den Mittelpunkt gestellt. Diese Analyse der Privacy-Arena, einer Konfliktzone, in welcher unterschiedliche Positionen zum Wandel von Privatheit aufeinandertreffen, wurde gestützt durch die Erschließung der Dichotomie von Privatheit und Öffentlichkeit. Hier wurde eine Expertise zu den Begriffen Privatheit und Öffentlichkeit erstellt. Weiterhin ging es um die Analyse des Wertes „Privatheit“ und des Wandels, dem dieser Wert, ausgelöst durch verschiedene gesellschaftliche Entwicklungen, unterworfen ist. Ferner wurden normative Ordnungen, die im Kontext des digitalen Wandels stehen und Privatheit definieren, analysiert. Ausgelöst durch die massenhafte Verbreitung informationstechnischer Systeme und deren weitreichenden Überwachungsmöglichkeiten ist es zu einer offensichtlichen Entgrenzung der Differenzierung von Privatheit und Öffentlichkeit gekommen.

Wird Privatheit über die Kontrolle definiert, welche eine Person über eigene personenbezogene Daten und Informationen hat, so wird diese Kontrolle den Nutzerinnen und Nutzern informationstechnischer Systeme sukzessive entzogen. Dementsprechend kommt es zu einer Neuaushandlung und Neubestimmung des Werts der Privatheit. Dabei wird deutlich, dass es keine dominante Privacy-Logik gibt, unter der alle Akteur_innen der Arena sich vereinen. Vielmehr entsteht eine Pluralität an Privatheitsbegriffen, deren normative Implikationen freigelegt werden müssen.

Verwendung der Zuwendung:

Die Zuwendung wurde überwiegend für folgende Positionen verwendet:

- Beschäftigungsentgelte für zwei wissenschaftliche Mitarbeiter
- Studentische Hilfskräfte
- Reisegelder für Projekttreffen

AP 2: Beschreibung der beteiligten bzw. betroffenen sozialen Welten und Rekonstruktion ihrer unterschiedlichen „Privacy-Logiken“

Ziele: Beschreibung der normativen Ordnungsmerkmale des Arena-Segments des Schengen-Routings sowie die Analyse von Entwicklungstendenzen in den beteiligten Welten.

Arbeitsschritte und erzielte Ergebnisse:

- Es wurden die durch die Soziologie erstellen Arena-Karten einer ethischen Reflexion unterzogen, bei welcher marginalisierte Positionen innerhalb der Konflikte um das Schengen-Routing herausgearbeitet wurden.
- Es wurden die normativen Positionen der Konfliktbeteiligten herausgearbeitet; dominante Positionen wurden in Kontrast gesetzt zu marginalisierten oder abwesenden Positionen. So sollte etwa beim Schengen-Routing eine Reterritorialisierung von Datenströmen unternommen werden, um sich vor der Telekommunikationsüberwachung nicht-europäischer Geheimdienste zu schützen. Dabei gäbe es jedoch auch praktikablere Möglichkeiten als ein nationales Routing, etwa die breitere Implementierung von Verschlüsselungsverfahren.
- Bei der Ausarbeitung der theoretischen Grundlegung zur normativen Bestimmung von Privatheit und Öffentlichkeit bzw. der Expertise zu den Begriffen Privatheit und Öffentlichkeit im Rahmen des zweiten Arbeitspaketes ist ein umfassendes Papier erarbeitet worden, welches die Ideengeschichte als auch unterschiedliche Begriffe, Konzepte und Theoriemodelle des Privaten und Öffentlichen beschreibt. Ausgehend von der griechischen Antike entwickeln sich unterscheidbare Traditionen und Theorien. Deren gemeinsamer Kern besteht darin, dass sie die „Privatsphäre“, häufig vorgestellt als „das (ganze) Haus“ und die Familie, in Abgrenzung zu dem bestimmen, was als Öffentlichkeit gilt. Damit beschreibt der Bereich des Privaten einen Sozialraum, welcher sich durch bestimmte Handlungsnormen und Konventionen konstituiert. Dieser Sozialraum steht in der Hauptsache in Relation zu drei weiteren gesellschaftlichen Sphären oder Feldern – zur eigenen Nah- oder Lebenswelt, zur Wirtschaft sowie zum Staat. Definitionen des Privaten spalten sich auf in solche, welche das Private negativ in Begriffen der Abspaltung, Einsamkeit, Vermeidung und des Rückzugs definieren und solche, welche das Private positiv durch Begriffe der Kontrolle und Freiheit definieren.

Räumliche Privatheitskonzepte betonen eher erstgenannte Begriffe und definieren Privatsphäre über den Schutz einer Person vor bestimmten sozialen "Inputs", während informationelle Privatheitskonzepte sich eher auf letztgenannte Begriffe berufen und Privatsphäre über die Kontrolle definieren, welche eine Person über soziale "Outputs" ausübt. Beiden Privatheitskonzeptionen ist im weitesten Sinne gemein, dass sie Privatheit als einen dialektischen Prozess definieren, welcher Zugangsbeschränkungen oder die "Permeabilität" zum eigenen "Selbst" entweder gezielt lockern oder verschärfen. Ergebnisse der Studie zum Wandel des Privaten finden sich im Kapitel „Privatheit – Ideengeschichte und theoretische Zugänge", in: B. Büttner, C. Geminn, T. Hagendorff, J. Lamla, S. Ledder, C. Ochs, F. Pittroff (2016): Die Reterritorialisierung des Digitalen. Zur Reaktion nationaler Demokratie auf die Krise der Privatheit nach Snowden. Kassel: kassel university press, 93-110.

Verwendung der Zuwendung:

Die Zuwendung wurde überwiegend für folgende Positionen verwendet:

- Beschäftigungsentgelte für zwei wissenschaftliche Mitarbeiter
- Studentische Hilfskraft
- Reisegelder für Projekttreffen und Konferenzen

AP 3: Analyse von Arena-Prozessen an exemplarischen Aushandlungsorten

Ziele: Analyse des Arena-Diskurses hinsichtlich artikulierter Problemdeutungen, kontroverser Positionen, hegemonial auftretender Privacy-Vorstellungen, überraschender Ortes des Schweigens, Wahrnehmungen und Rechtfertigungen von Exklusions- und Inklusionseffekten.

Arbeitsschritte und erzielte Ergebnisse:

- Obwohl im Antrag nicht explizit geplant, fiel die Entscheidung darauf, einen Teil der Forschung des Teilprojekts Ethik/Philosophie auf den Begriff des Vertrauens zu fokussieren. Der Grund dafür ist, dass im Lauf der Forschung deutlich wurde, welche zentrale Rolle Vertrauen bzw. Systemvertrauen in die Infrastruktur des Internets bei deren Benutzung spielt und inwiefern Misstrauen zu Vermehrung von Kontroll- und Prüfaufgaben führt, um Informationssicherheit herzustellen. Damit wurde die Arbeit von AP 1 aufgenommen und weitergeführt. Der Begriff des Vertrauens liegt quer zu diversen Themenkomplexen. Die durch die Snowden-Enthüllungen initiierte breite Thematisierung bislang geheimer nachrichtendienstlicher Tätigkeiten in der Öffentlichkeit hat die Vorstellungen darüber, welche Bedeutung das Internet bei der staatlichen Überwachung spielt, drastisch verändert. Es besteht nun ein breites Wissen darüber, dass das technisch Mögliche zur Überwachung und Ausspähung der digitalen Welt weitestgehend ausgeschöpft wird. Dies hat einen Vertrauensverlust innerhalb der Bevölkerung zur Folge, welcher die Geheimdienste, die Regierungen insgesamt, aber auch die Internetkonzerne betrifft. Die Vertrauenskrise hat bereits ökonomische Konsequenzen – wie etwa an den monetären Verlusten amerikanischer Cloud-Anbieter zu erkennen ist; zugleich aber verändert sie die politische und wirtschaftliche Diskursführung. Eben weil die Snowden-Enthüllungen ein starkes Misstrauen gegenüber den Akteuren der Überwachung initiiert haben, wird der Versuch sichtbar, den Vertrauensverlust durch eine Vertrauensrhetorik auszugleichen. Vertrauen wird zum Werbewort. Trotz einer breiten „Vertrauens-

Rhetorik“ hat das Internet seinen Charakter als offenes System einer globalen Kommunikationsgemeinschaft verloren. Die Sicherheitsstrukturen des zivilen Internets sich durch geheimdienstliche Tätigkeiten weitestgehend unterminiert worden. Als Reaktion darauf werden Forderungen nach der breiten Implementierung von Datenschutz-, Anonymisierungs- und Verschlüsselungstechnologien in Internetapplikationen sowie nach der Einführung nationaler Netze laut, damit die „Hoheit“ über Datenströme gewahrt werden kann. Es geht um technische Maßnahmen, die ausländischen Geheimdiensten den Zugriff auf jene Datenströme zu erschweren oder unmöglich machen sollen. Die Wahrnehmung einer Fragmentierung des Netzes in bestimmte Server- und Routingräume, wovon die einen als „vertrauenswürdig“ und die anderen als „kompromittiert“ gelten, ist auch als Folge der Tatsache zu werten, dass Gesetze keine exterritoriale Wirkung haben und Datenströme innerhalb eines bestimmten Rechtsrahmens unter Kontrolle gehalten werden sollen. Innerhalb dieses vertrauten Datenraumes sollen Überwachungs- und Spionagetätigkeiten restringiert oder ganz verboten werden. Darüber hinaus geht es darum, ein einheitliches Niveau des Datenschutzes sicherzustellen und Daten stets dem gleichen gesetzlichen Rahmen unterwerfen zu können.

- Der Diskurs der Privacy-Arena wurde aus einer ethischen Perspektive beleuchtet. Dabei wurde für die an der Arena beteiligten Welten, also die Welt des Staates, die Welt des Rechts, die Welt der Geheimdienste, die Welt der Unternehmen und die Welt der Netzgemeinde jeweils eine Bestimmung und Gewichtung der darin artikulierten Positionen unternommen. Der Fokus lag hier insbesondere darauf, die unterschiedlichen Privacy-Logiken der Akteur_innen in der Arena zu beschreiben. Ein erster Befund war, dass innerhalb der Privacy-Arena keine solche Logik als dominante Führungsgröße auftritt, sondern differente Positionen zum Wandel von Privatheit nebeneinander bestehen.
    - In der Welt des Staates wird der Begriff des Privaten häufig als rhetorische Formel gebraucht, ohne dass weiter spezifiziert würde, welche Art von Privatheit gemeint ist. Die Funktion von Privatheit wird mitunter darin gesehen, die Macht des Staates zu limitieren. Privatheit steht damit in einem engen Zusammenhang mit dem Grundrecht auf die freie Entfaltung der Persönlichkeit. Dieses Grundrecht reguliert, wie weit der Staat in die Lebenswelt der Bürger eindringen darf. Dabei geht es nicht um ein räumliches Eindringen der Exekutive in private Bereiche, sondern vielmehr um eine Limitation staatlicher, personenbezogener Datenerhebungsverfahren, welche durch den Grundrechtsschutz der informationellen Selbstbestimmung adressiert wird. Politische Forderungen nach dem Schutz der Privatsphäre können Zügelungsversuche sein, welche an die Geheimdienste gerichtet sind.
    - In der Welt der Geheimdienste wird der Wert des Privaten in ein Spannungsfeld zum Wert der Sicherheit gestellt. Dieses Spannungsfeld wird als Nullsummenspiel verstanden, sodass sich zwischen Privatheit und Sicherheit ein Konflikt entfaltet und entweder der eine oder der andere Wert dominiert, ohne dass Privatheit und Sicherheit gleichzeitig hergestellt werden könnten. Geheimdienste berufen sich auf den Bemäntelungseffekt der Privatsphäre. Die Privatsphäre, so sehen es Geheimdienste, ist gleichsam eine Sphäre der Vorbereitung und

Ausübung krimineller oder terroristischer Tätigkeiten. Die Privatsphäre wird als eine Art Schild interpretiert, welches dazu dienen kann, Straftaten zu verschleiern.

- In der Welt des Rechts schließlich wird versucht, das Niveau der rechtlichen Regulierungsdichte den sich rasant vollziehenden technologischen Entwicklungen anzupassen.
- In der Welt der Netzgemeinde geht es, ähnlich wie in der Welt des Rechts, vornehmlich um den Wandel der informationellen Privatheit. Innerhalb der Netzgemeinde werden Forderungen nach einem Schutz der Privatsphäre zumeist als Forderungen nach strengeren Datenschutzmaßnahmen vorgetragen. Diese betreffen Methoden der Gewinnung, Verarbeitung und Verbreitung von Daten in der Welt des Staates und der Unternehmen.
- Die Welt der Unternehmen, benutzt den Begriff des Privaten, ähnlich wie die Akteure in der Welt des Staates, überwiegend als rhetorische Formel respektive als Werbewort. Wer die Privatsphäre bzw. genauer den Schutz der Daten seiner Kund_innen sicherstellt, kann sich davon Wettbewerbsvorteile erwarten. Es geht um die Herstellung eines gewissen Vertrauensniveaus von Kund_innen hinsichtlich der informationstechnischen Integrität von Unternehmen.

- Die Ergebnisse sind unter anderem im gemeinsamen Aufsatz über die „Reterritorialisierung des Netzes und ihrer demokratischen Alternativen“ zusammengefasst. Er findet sich unter „Die Verlaufskurve des nationalen Routings und die Reproduktion der Container-Gesellschaft“, in: B. Büttner, C. Geminn, T. Hagendorff, J. Lamla, S. Ledder, C. Ochs, F. Pittroff (2016): Die Reterritorialisierung des Digitalen. Zur Reaktion nationaler Demokratie auf die Krise der Privatheit nach Snowden. Kassel: kassel university press, 145-152. Hier wurde untersucht, welchen Stellenwert eine Reterritorialisierung von Datenströmen vor dem Hintergrund der Vertrauenskrise gegenüber digitalen Medien hat, welche Folgen mit der Arena-Politik rund um die Idee des Schengen-Routings einhergehen und welche alternativen demokratiepolitischen Reaktionsweisen es auf die Snowden-Enthüllungen geben könnte.

Verwendung der Zuwendung:

Die Zuwendung wurde überwiegend für folgende Positionen verwendet:

- Beschäftigungsentgelte für zwei wissenschaftliche Mitarbeiter
- Studentische Hilfskraft
- Reisegelder für Projekttreffen und Konferenzen

AP 4: Zusammenführung und Verdichtung von Hypothesen zur Privacy-Arena und ihrer gesellschaftlichen Entwicklung

Ziele: Erstellung einer gemeinsamen Buchpublikation zum Abschluss des Projekts.

Arbeitsschritte und erzielte Ergebnisse:

- Es wurden die Arbeiten aus der ersten Projektphase zusammengetragen, nochmals gemeinsam diskutiert, und letztlich in einer Buchpublikation festgehalten: B. Büttner, C. Geminn, T. Hagendorff, J. Lamla, S. Ledder, C. Ochs, F. Pittroff (2016):

Die Reterritorialisierung des Digitalen. Zur Reaktion nationaler Demokratie auf die Krise der Privatheit nach Snowden. Kassel: kassel university press

Verwendung der Zuwendung:

Die Zuwendung wurde überwiegend für folgende Positionen verwendet:

- Beschäftigungsentgelte für zwei wissenschaftliche Mitarbeiter
- Studentische Hilfskraft
- Reisegelder für Projekttreffen und Konferenzen

2.1.2 Arbeitspakete des Verlängerungsantrags

AP 1: Privatheit und Demokratie

Ziele: Ziel des ersten Arbeitspakets ist die Auswahl thematischer Problemfelder (Issues) sowie daran Analysen der Governance-Strukturen der jeweiligen Issues.

Arbeitsschritte und erzielte Ergebnisse:

- Beim ersten Projekttreffen der Verlängerungsphase wurden vier Themenbereiche („Issues“) für eine vertiefte Bearbeitung in Ausblick genommen: Big Data, Kryptografie, Sousveillance und Wearables.
- Im weiteren Projektfortschritt und insbesondere für den Kontext der Abschlussveröffentlichung und der Ausstellung fand eine Konzentration auf die Issues Big Data, Kryptografie, Sousveillance statt, da die Dringlichkeit und Komplexität dieser Bereiche für die Bearbeitung vordringlich erschien.
- Alle drei Gegenstandsbereiche sind auf je eigene Weise mit Machtverhältnissen befasst. Als Grundlage für deren Analyse wurde ein Konzept ko-konstitutiver Macht erarbeitet, das auf unterschiedlichen existenten Machtverständnissen aufbaut. Es schließt an relationale und damit nicht Fähigkeiten- oder ressourcenbasierte Machtverständnisse an. Die Machtbeziehungen nach einem ko-konstitutiven Verständnis wiederum verstehen sich nicht als einseitige Wirkzusammenhänge, sondern als strukturelle oder bedeutungsbezogene Zusammenhänge. Damit setzen sie bei Foucaults Arbeiten zur Bedeutung des Diskurses für soziale Beziehungen und an materialistische Verständnisse von strukturellen Rahmenbedingungen für soziale Beziehungen an. Der Vorteil eines solchen Verständnisses liegt für die Themen von Big Data, Kryptografie und Sousveillance v.a. darin, auch Technik als Teil von grundlegenden strukturellen und normsetzenden Machtbeziehungen zu verstehen. Zum einen ermöglicht dieser Ansatz die Einbeziehung der Technik in soziale Analysen, zum anderen werden durch die Analyse von Machtstrukturen auch Governance-Analysen virulent; darüber hinaus werden normative Implikationen von Technik, implizite Werte und grundsätzlich demokratierelevante Machtverschiebungen analysierbar gemacht. Dieses Machtverständnis diente bei der Bearbeitung der Issues und Segmente als grundlegende Vergleichsfolie. Die Ergebnisse finden sich u. a. in Baur-Ahrens, Andreas (2017): „The power of cyberspace centralisation: analysing the example of data territorialisation“, in: Matthias Leese und Stef Wittendorp (Hg.) *Security/Mobility. Politics of Movement*, Manchester: Manchester University Press, 37–56.

Verwendung der Zuwendung:

Die Zuwendung wurde überwiegend für folgende Positionen verwendet:

- Beschäftigungsentgelte für zwei wissenschaftliche Mitarbeiter
- Studentische Hilfskraft
- Reisegelder für Projekttreffen und Konferenzen

AP 2: Analyse der vier weiteren Arena-Segmente

Ziele: Analyse der Arenaprozesse innerhalb der Aushandlungen rund um die EU-Datenschutz-Grundverordnung, Bundestagsausschüsse, die NETmundial-Konferenz sowie Wirtschaftsdialoge.

Arbeitsschritte und erzielte Ergebnisse:

- Anhand verschiedener Demokratiemodelle wurde untersucht, welche Governance-Strukturen sich innerhalb der Aushandlungsorte bezüglich der drei Themenschwerpunkte Big Data, Kryptografie und Sousveillance. Mit Hilfe unterschiedlicher Demokratiemodelle wurde untersucht, welche Governance-Modelle sich in Bezug auf diese drei Gegenstandsbereiche manifestieren. Erarbeitung der ethischen Problemstellungen der Issues Kryptografie, Big Data und Sousveillance. Außerdem Analyse der Art und Weise, wie in den vier Segmenten (EU-Datenschutz-Grundverordnung, Bundestagsausschüsse, die NETmundial-Konferenz, Wirtschaftsdialoge) auf die jeweiligen Problemstellungen reagiert wurde. Während das Thema Sousveillance im Kontext verschiedener Publikationen abgehandelt wurde (z.B. Hagendorff 2017), fanden gesonderte Ausarbeitungen zu Kryptografie und Big Data für die Privacy-Ausstellung in Kassel und die Netzseiten zu den Ergebnissen des Projekts statt, die hier gekürzt und exemplarisch vorgestellt werden (ausführlicher Text und bibliografische Angaben im Anhang):

- **Kryptografie**
  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 nebeneinanderstehen.

[…]

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.

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 2051).

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.

[…]

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.

- **Big Data**

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 Awendungsmöglichkeiten, Hoffnungen und Kritk – einen Hype, einen regelrechten ‚Datenrausch'.

[…]

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 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.

Fehlende Kontextualität und Intransparenz von Big-Data-Analysen

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. *[…]* „[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.

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).

Verwendung der Zuwendung:

Die Zuwendung wurde überwiegend für folgende Positionen verwendet:

- Beschäftigungsentgelte für zwei wissenschaftliche Mitarbeiter
- Studentische Hilfskraft
- Reisegelder für Projekttreffen und Konferenzen

AP 3: Dekontextualisierung und Kontrolle von Information

Ziele: Untersuchung darüber, welche Auswirkungen die zunehmende Auflösung von informationellen Kontextbarrieren durch digitale Technologien und die daran anschließende Freisetzung von Informationsflüssen auf das Verständnis des Privaten hat.

Arbeitsschritte und erzielte Ergebnisse:

- Analyse darüber, inwiefern sich der Begriff der informationellen Privatheit letztlich auf Fragen der gelingenden Kontrolle hinsichtlich personenbezogener Informationen zurückführen lassen kann
- Analyse der Folgen des Verlusts der Informationskontrolle nebst den damit verbundenen Auswirkungen dieses Verlusts auf den Privatheitsschutz, das individuelle Identitätsmanagement sowie Transparenzniveaus. Ausführliche Ergebnisse finden sich in Hagendorff, Thilo (2017): Das Ende der Informationskontrolle. Bielefeld: Transcript, insbesondere in den Kapiteln „Privatheit", „Identitätsmanagement" und „Transparenz".
- Es wurde eine Theorie der Informationskontrolle ausgearbeitet. Diese Theorie subsummiert Diskurse rund um Datenschutz und Privatheit unter den Aspekt der Kontrolle personenbezogener Informationen innerhalb verschiedener sozialer Kontexte. Gefragt wird, wie diese Kontrolle ausgeübt wird, warum sie wichtig ist und inwiefern der digitale Wandel vorhandene Kontrollmöglichkeiten beeinflusst. Dabei wird unter anderem gezeigt, wie auf verschiedenen Ebenen – also etwa der der materiellen Infrastruktur des Internets, der der Codes, Algorithmen und Protokolle oder der der Benutzerschnittstellen – der Versuch gemacht wird, Informationen zu kontrollieren. Damit die informationelle Privatheit einer Person gesichert werden kann, muss diese Person, so die Theorie, in der Lage sein, zum einen den Zugang von Dritten zu persönlichkeitsrelevanten Informationen einschränken und zum anderen die Verteilung jener Informationen kontrollieren zu können. Informationelle Privatheit soll als eine bestimmte Organisation der Distribution von Informationen und somit als erfolgreiche Informationskontrolle beschrieben werden. Hierbei wird im Wesentlichen zwischen drei Formen der Informationskontrolle differenziert: Es geht (1) um die Wahl, welche Informationen in welchen Situationen mitgeteilt und verbreitet werden dürfen (choice). Es geht (2) um die Zustimmung einzelner Personen, dass auf sie bezogene Informationen zwischen Akteuren transferiert und verbreitet werden dürfen (consent). Und es geht (3) um die Möglichkeit, auf Informationsbestände, welche etwa in Datenbanken gespeichert sind, zugreifen und diese im Bedarfsfall korrigieren zu können (correction). Alle drei Formen der Informationskontrolle – also die Wahl, welche Informationen erhoben und verbreitet werden, die Zustimmung über die Verbreitung von Informationen sowie die Möglichkeit zur Korrektur fehlerhafter Informationsbestände – sind Teil der Idee des fairen Informationsmanagements und der informationellen Privatheit. Faktisch jedoch verfügen private Endnutzer_innen digitaler Kommunikationstechnologien und Plattformen in der Regel über keine der genannten Formen der Informationskontrolle. Für sie ergeben sich Kontrollmöglichkeiten über die Erhebung, Verarbeitung und Verbreitung von Daten nur bedingt, vermittelt über Benutzerschnittstellen. Sie agieren an einer Oberfläche technischer Artefakte, deren „Maschinenräume" sie in der Regel nie einsehen, geschweige denn verstehen werden. Aus dieser Perspektive besitzen digitale Medien eine radikale Intransparenz. Das Design digitaler Medien ist darauf ausgelegt, dass auf der Ebene der Benutzerschnittstellen, der Graphical User

Interfaces (GUI) nicht mehr erkannt werden soll, was sich „dahinter“ abspielt. Akteu_innen allerdings, welche nicht an die Ebene der Benutzeroberflächen gebunden sind, sondern welche sich „dahinter“, also auf die Ebene der Codes, Algorithmen und Protokolle begeben können, können Computer nahezu für beliebige Zwecke einsetzen, während dieser Möglichkeitsraum für Endnutzer_innen auf die begrenzte Bandbreite bereitgestellter „Features“ von informationstechnischen Systemen und Plattformen zusammenschrumpft. Gegenüber Hacker_innen, Softwareingenieur_innen, Informatiker_innen etc. manifestiert sich für durchschnittliche Endnutzer_innen ein radikales „Nichtkönnen“, da sie nicht einsehen oder gar kontrollieren können, was in der „Tiefe“ der Datenverarbeitungsprozesse informationstechnischer Systeme passiert. Diese Intransparenz informationstechnischer Systeme ist jedoch nur einer von vielen Faktoren, welche Treiber des informationellen Kontrollverlusts sind. Aufbauend auf jener Intransparenz agieren Hacker_innen, welche von der Allgegenwart an Sicherheitslücken in Informations- und Kommunikationstechnologien profitieren und diese ausnutzen. Ebenfalls profitieren Geheimdienste, welche nichts weniger als die nahezu totale Überwachung der globalen elektronischen Telekommunikation anstreben. Dies verbindet sich mit der routinierten Missachtung von Datenschutzgesetzen durch die Geschäftspraxis diverser IT-Unternehmen. Ferner kommt die Entwicklung neuer digitaler Medien und neuer Plattformen hinzu, welche jeweils dem Prinzip der Datensparsamkeit, des Privacy by Design oder des Privacy by Default entgegenstehen. Zwar werden Technikentwickler_innen als Regelungsadressat_innen angesprochen werden, um datenschutzkonforme Techniken zu entwerfen und diese mit datenschutzkonformen Defaulteinstellungen zu versehen; dennoch steht der Datenschutz, darunter insbesondere das Prinzip der Datensparsamkeit, einer Gesellschaft, deren Innovationsfaktor und Grundsubstanz Daten als Träger von Informationen sind, konträr gegenüber. So werden die Kämpfe um den Erhalt der kontextuellen Integrität, um Datenschutz und Privatheit inzwischen folgerichtig als „Rückzugsgefechte“ betitelt. Es scheint, als ließen sich nur mit größten Schwierigkeiten valide Mechanismen zur Kontrolle von Daten- und Informationsströmen im Kontext digitaler Technologien finden. Allerdings wäre gerade dies die Voraussetzung dafür, sozial etablierte Informationskontexte in einer zunehmend digitalisierten Gesellschaft weiterhin erhalten zu können. Darin aber spielt sich der soziale Wandel in der Informationsgesellschaft ab: in der langsamen Auflösung von originär ausdifferenzierten Informationskontexten. Im Kleinen bildet er sich durch das abrupte Kollabieren von Informationskontexten ab, beispielsweise durch einschlägige Leaks geheimer Informationen oder durch spektakuläre Hackerangriffe auf Internetplattformen. In der Gesamtschau jedoch zeigt sich ein eindeutiger Trend, nämlich die nachhaltige Entdifferenzierung etablierter Informationskontexte. Dieser Entdifferenzierungsprozess eigentlich getrennter Informationskontexte zeitigt „medienpanische Diskurse“, welche sich aktuell vorrangig um Themen wie die Auflösung des Privaten, die Verletzung des Datenschutzes oder die Aufhebung von Informationssicherheit drehen. Letztlich aber wirkt jedes neue Verbreitungsmedium, welches in eine Gesellschaft integriert wird – sei dies die Schrift, der Buchdruck, die Fotografie, das Fernsehen oder der Computer –, als ein Auslöser von Ängsten, Dramatisierungen, Protesten und Kontrollverlustereignissen. In „medienpanischen Diskursen“ werden neue

Verbreitungsmedien moralisch verurteilt für ihr Potential, etablierte soziale oder kulturelle Normen der Informationsverbreitung und des Informationsflusses zu bedrohen oder zu zersetzen. Ein Kennzeichen jener „medienpanischen Diskurse“ ist dabei, dass es eine Art geschichtliche Vergesslichkeit gibt, sodass jedes neue Verbreitungsmedium auch erneut Auslöser von medienpanischen Diskursen ist, ungeachtet der strukturellen Gleichheit dieser Diskurse mit vorhergehenden. Neue Verbreitungsmedien – im aktuellen Fall der Computer – irritieren, allgemein gesprochen, die kulturelle Praxis einer Gesellschaft. Der Medienwandel, der digitale Strukturwandel und die entsprechenden Kulturreformen bergen ebenso Gefahren wie Chancen, wobei nicht letztgültig zu entscheiden ist, ob eher erstere oder letztere gewichtiger sind. Dennoch werden vielerorts die Gefahren eher gesehen als die Chancen. Dies erklärt sich dadurch, dass derzeit eine Phase des „Chaos“ vorherrscht, welche sich wesentlich durch informationelle Kontrollverlustereignisse, also das sich gegenseitige Durchdringen von traditionell getrennten Informationskontexten auszeichnet. Klassischerweise wird zwischen zwei Informationskontexten differenziert, nämlich dem Privaten und dem Öffentlichen. In Erweiterung dieser grundlegenden Differenzierung können diverse weitere Ausdifferenzierungen verschiedener Informationskontexte beobachtet werden, worunter beispielsweise verschiedene Freundeskreise, Familien- oder Verwandtschaftsverbände ebenso zu zählen sind wie Firmenabteilungen, Arztpraxen oder Schulklassen. Informationskontexte besitzen, bildlich gesprochen, an ihren Rändern Grenzen, welche Informationen nicht beliebig übertreten können oder sollen. Jene Informationskontexte jedoch, sofern sie sich in sozialen Systemen aufspannen, welche vom Trend der Digitalisierung erfasst werden, erfahren eine zunehmende Aufweichung durch vernetzte informationstechnische Systeme, wobei diese Aufweichung insbesondere normativ über den Begriff des Privaten problematisiert wird. Die informationelle Privatheit wird, wie beschrieben, über die erfolgreiche Kontrolle des Verbreitungsradius von personenbezogenen Informationen gesichert. Dabei verhalten sich die Normen der angemessenen Informationsverbreitung und damit die Normen zur Bestimmung des Privaten relativ zu bestimmten Kulturen oder zeitlichen Epochen. Der soziale Wandel, welcher durch die steigende Dichte untereinander vernetzter, stets in ihrer Leistungsfähigkeit anwachsender Informations- und Kommunikationstechnologien angestoßen wird, beschreibt gleichsam eine steigende „Liquidität“ und „Autonomie“ von Informationsströmen. Informationen verbreiten sich stets „ungehemmter“, beschleunigter und ortsungebundener. Die informationelle Selbstbestimmung, also die Kontrolle über personenbezogene Informationen, wird allgemein als wichtiges Gut erachtet, welches im Zentrum der Idee des Privaten, des Datenschutzes oder der Informationssicherheit steht, welches aber auch soziale Praktiken des Identitätsmanagements und der Selbstdarstellung fundamental betrifft. Sofern es Personen jedoch nicht mehr möglich ist, Informationen, welche sie selbst betreffen, so zu kontrollieren, dass verschiedene soziale und institutionelle Kontexte sowohl auf einer der Gesellschaft informationell voneinander getrennt werden können, kann dies zu schweren Irritationen des Identitätsmanagements und der eigenen Persönlichkeitskonstitution führen. Dennoch ist der informationelle Kontrollverlust nebst den Risiken der diversen negativen Konsequenzen, welche aus ihm erwachsen können, eine zentrale Eigenschaft moderner Informationsgesellschaften. Im Anschluss daran stellt sich die Frage nach

Strategien, nach Formen der Resilienz, welche gegenüber den Risiken informationeller Kontrollverlustereignisse eingenommen werden können. Die Unmöglichkeit, als Endnutzer_in mit informationstechnischen Systemen so umzugehen, dass kontrolliert oder auch nur überblickt werden kann, wie und in welchem Umfang Daten, welche als Träger von personenbezogenen Informationen fungieren, erhoben, verarbeitet und verbreitet werden, erfordert ein neues Paradigma der Mediennutzung und der Medienkompetenz; darüber hinaus wirkt dieser Kontrollverlust bis in elementare Bereiche des persönlichen Identitätsmanagements und der Selbstdarstellung hinein. Der Kontrollverlust gibt Anlass, aus Gründen der Resilienz gegenüber dem „context collapse" neue Weisen des digitalen Identitätsmanagements einzuüben. Diese neuen Formen des digitalen Identitätsmanagements sind in der Lage, das Kollabieren von Informationskontexten nicht mehr als Enttäuschung, als Verletzung sozialer Normen des angemessenen Informationsflusses wahrzugenommen, sondern es zu erwarten. Sobald computervermittelte Kommunikationszusammenhänge nicht mehr von Normen der Privatheit, des Datenschutzes, des restringierten, in klaren Bahnen gelenkten „Fließens" von Informationen bestimmt wird, sondern der informationelle Kontrollverlust selbst zu Normalität und zur Norm wird, werden nur jene Formen der Mediennutzung adäquat sein, welche nicht mehr vom Bestehen unterschiedlicher geschlossener Kontexte ausgehen, innerhalb derer Informationen ausschließlich und exklusiv zirkulieren, innerhalb derer verschiedene Kommunikationsstile gepflegt werden und innerhalb derer sich verschiedene Modi der Selbstdarstellung niederschlagen.

Verwendung der Zuwendung:

Die Zuwendung wurde überwiegend für folgende Positionen verwendet:

- Beschäftigungsentgelte für zwei wissenschaftliche Mitarbeiter
- Studentische Hilfskraft
- Reisegelder für Projekttreffen und Konferenzen

AP 4: Visuelle Kommunikation

Ziele: Visualisierung der Privacy-Arena im Rahmen eines Kunstprojekts

Arbeitsschritte und erzielte Ergebnisse:

- Mitarbeit bei der Erstellung einer Kunstausstellung, in welcher anhand verschiedener Stationen die gewählten Issues bzw. Segmente der Privacy-Arena in ein ästhetisches Produkt transformiert wurden.
- Häufige Projekttreffen und Skype-Telefonate mit den Künstler_innen, um gemeinsam die Inhalte der Arbeiten in Kunstinstallationen umzusetzen.
- Erstellung von Texten für einen ausstellungsbegleitenden Katalog.

Verwendung der Zuwendung:

Die Zuwendung wurde überwiegend für folgende Positionen verwendet:

- Beschäftigungsentgelte für zwei wissenschaftliche Mitarbeiter
- Studentische Hilfskraft
- Reisegelder für Projekttreffen und den Besucht der Kunstausstellung in Kassel

AP 5: Methodenreflexion

Ziele: Reflexion der in der Soziologie sowie den Rechtswissenschaften gewählten Methoden.

Arbeitsschritte und erzielte Ergebnisse:

- Insbesondere während der Projekttreffen fand eine Reflexion der Methoden statt, anhand welcher innerhalb der Rechtswissenschaften sowie der Soziologie Arena-Analysen vorgenommen wurden. Hierbei wurde insbesondere das Instrumentarium der soziologischen Kartografie von Arenen kritisch diskutiert.

Verwendung der Zuwendung:

Die Zuwendung wurde überwiegend für folgende Positionen verwendet:

- Beschäftigungsentgelte für zwei wissenschaftliche Mitarbeiter
- Studentische Hilfskraft
- Reisegelder für Projekttreffen

AP 6: Zusammenführung der Ergebnisse

Ziele: Zusammenführung der Forschungsergebnisse von allen Projektpartnern in Vorbereitung einer gemeinsamen Publikation zum Abschluss des Projekts

Arbeitsschritte und erzielte Ergebnisse:

- Erstellung einer gemeinsamen Abschlusspublikation. Im Vorfeld der Abschlusspublikation wurde bereits eine Broschüre, welche die Kunstausstellung begleitete, mitentwickelt.

Verwendung der Zuwendung:

Die Zuwendung wurde überwiegend für folgende Positionen verwendet:

- Beschäftigungsentgelte für zwei wissenschaftliche Mitarbeiter
- Studentische Hilfskraft
- Reisegelder für Projekttreffen

AP 7: Publikation

Ziele: Eine gemeinsame Publikation der Forschungsergebnisse zur Privacy-Arena soll den Abschluss des Projekts bilden.

Arbeitsschritte und erzielte Ergebnisse:

- Zusammenstellung einzelner Texte.
- Finale Redaktion und Veröffentlichung der Abschlusspublikation.

Verwendung der Zuwendung:

Die Zuwendung wurde überwiegend für folgende Positionen verwendet:

- Beschäftigungsentgelte für zwei wissenschaftliche Mitarbeiter
- Studentische Hilfskraft
- Reisegelder für Projekttreffen

2.2 Die wichtigsten Positionen des zahlenmäßigen Nachweises

Vorweg soll noch einmal darauf hingewiesen werden, dass in Rücksprache mit dem Projektträger kleinere Umschichtungen im Budget gab, die die veränderten Anforderungen

im Laufe der Projektdauer widerspiegeln. Der genaue zahlenmäßige Nachweis liegt dem Projektträger bereits vor und soll hier nur exemplarisch aufgegriffen werden.

Position 0812 (Beschäftigte E12-E15):

Aus Position 0812 wurden die Beschäftigungsentgelte für die zwei wissenschaftlichen Angestellten gezahlt TV-L E13. Die genaue Aufstellung der Posten sind im zahlenmäßigen Nachweis aufgelistet. Für die Bearbeitung aller Arbeitspakete waren dies:

- Andreas Baur-Ahrens
- Dr. Thilo Hagendorff
- Jutta Krautter
- Simon Ledder
- Maria Pawelec

Position 0822 (sonstige Beschäftigungsentgelte):

Aus Position 0822 wurden die Beschäftigungsentgelte für die wissenschaftliche Hilfskraft gezahlt, welche die Arbeiten innerhalb des Projekts unterstützte. Dies war in wechselnder Besetzung:

- Milan Babic: 5 Monate studentische Hilfskraft (ungeprüft) 20 Stunden pro Monat / 2 Monate studentische Hilfskraft (geprüft) 20 Stunden pro Monat
- Alexander Hauschild: 18 Monate studentische Hilfskraft (geprüft) 40 Stunden pro Monat

Position 0843

Aus Position 0843 wurden die Kosten für Büro- und Informationsmaterial gedeckt, außerdem Druckkosten und Materialkosten für die Kunstausstellung

Position 0846

Aus Position 0846 wurden zum einen die Kosten für Reisen zu Konferenzen gezahlt. Eine Auswahl der besuchten Konferenzen werden hier aufgeführt

- Andreas Baur-Ahrens, Reise nach Bielefeld und Berlin zu den Konferenzen: „Privatheit und Freiheit“ (Bielefeld), „re:publica“ und „Can we have some privacy“ (Berlin) (Mai 2015)
- Thilo Hagendorff, Reise nach Berlin zum Workshop „Privacy, Datenschutz & Surveillance“ (Dezember 2015)
- Thilo Hagendorff, Reise nach Leipzig zur Konferenz „Diskurs der Daten“ (Februar 2016)
- Thilo Hagendorff, Reise nach Aachen zur Konferenz „Daten\Gesellschaft!?“ (März 2016)
- Thilo Hagendorff, Reise nach Fribourg zur Jahrestagung der Schweizer Gesellschaft für Kommunikations- und Medienwissenschaft (April 2016)

Ferner wurden aus den Reisekosten die Projekttreffen gezahlt, welche abwechselnd in Kassel und Tübingen (hier fielen dann naturgemäß für das ethisch-philosophische Teilprojekt keine Kosten an) abgehalten wurden. Die Projekttreffen fanden circa vier Mal jährlich statt und wurden jeweils durch beide Mitarbeiter im Projekt besucht.

2.3 Die Notwendigkeit und Angemessenheit der geleisteten Arbeit

Das Projekt hat sich aufgrund der interdisziplinären Bearbeitung der Forschungsfragen als sehr fruchtbar erwiesen. Durch die Forschung konnten wichtige Erkenntnisse nicht nur in der Privatheitsforschung erarbeitet werden, sondern auch der wissenschaftliche Diskurs rund um das Thema Datenschutz vorangetrieben werden. Die Vorstellung der erarbeiten Ergebnisse auf Konferenzen zeigt, dass die im Projekt geleisteten Arbeiten in der wissenschaftlichen Community relevant sind. Zudem konnte neben der Abschlusspublikation aus der ersten Projektphase eine zusätzliche Monografie aus dem Forschungsprojekt heraus entstehen, welche 2017 veröffentlicht wurde. Auch wurden Mitarbeiter des Projekts immer wieder für Workshops, Seminare und Lehrveranstaltungen angefragt, um wissenschaftliche Erkenntnisse aus dem Projekt auch in anderen Kontexten als nur dem von wissenschaftlichen Forschung vorzustellen.

2.4 Der voraussichtliche Nutzen, insbesondere die Verwertbarkeit des Ergebnisses im Sinne des fortgeschriebenen Verwertungsplans

Wissenschaftliche Erfolgsaussichten nach Projektende:

Einschlägige Projektergebnisse werden in den beiden Abschlusspublikationen, in einer zusätzlichen Monografie sowie in zahlreichen Aufsätzen in Zeitschriften und Sammelbänden festgehalten. Da es sich beim Projekt Privacy-Arena um ein sozialwissenschaftlich-ethisches Projekt handelt, sind keine im engeren Sinne direkten wirtschaftlichen und/oder technischen Erfolgsaussichten zu erwarten. Dessen ungeachtet war das Projekt die Basis für zahlreiche Lehrveranstaltungen und Workshops, welche auch nach Projektende noch weitergeführt werden beziehungsweise neu entwickelt werden, jedoch auf Forschungsergebnissen der Privacy-Arena aufbauen.

2.5 Während der Durchführung des Vorhabens dem Zuwendungsempfänger bekannt gewordener Fortschritt auf dem Gebiet des Vorhabens bei anderen Stellen

Während der Durchführung des Vorhabens fanden parallel im Projekt Forum Privatheit (ebenfalls ein BMBF-Projekt) Forschungen statt. Hier ergab sich, auch durch nahen personellen Kontakt, ein intensiver Austausch, von dem beide Forschungen profitiert haben. Darüber hinaus fand während der Laufzeit im DFG-Graduiertenkolleg 1681/2 Privatheit und Digitalisierung sowie am Lehrstuhl von Prof. Dr. Christoph Gusy in Bielefeld Privatheitsforschung statt. Die Publikationen und Aktivitäten der anderen Projekte wurden intensiv zur Kenntnis genommen; die Schwerpunktsetzungen waren jedoch andere, sodass sich hier keine signifikanten Redundanzen in der Forschungsarbeit und hinsichtlich der Forschungsergebnisse ergeben haben. Vielmehr dienten die Forschungsergebnisse insbesondere des Forum Privatheit als gute Ergänzung der Arbeiten in der Privacy-Arena.

2.6 Erfolgte und geplante Veröffentlichungen der Ergebnisse

Publikationen:

- Baur-Ahrens, Andreas, Thilo Hagendorff und Maria Pawelec (2017): „Kryptografie“ sowie „Big Data“, in: Joel Baumann und Jörn Lamla (Hg.) *Privacy Arena: Kontroversen um Privatheit im digitalen Zeitalter*, Kassel: kassel university press, 44–57, 97–116.

- Baur-Ahrens, Andreas (2017): „The power of cyberspace centralisation: analysing the example of data territorialisation“, in: Matthias Leese und Stef Wittendorp (Hg.) *Security/Mobility. Politics of Movement*, Manchester: Manchester University Press, 37–56.
- Baur-Ahrens, Andreas et al. (2016): „Smart Technologies – Workshop on Challenges and Trends for Privacy in a Hyper-connected World“, in: David Aspinall et al. (Hg.) *Privacy and Identity Management. Time for a Revolution?*, IFIP AICT 476, Cham: Springer, 111–28.
- Baur-Ahrens, Andreas (2016): „Cyberwar“, in: Jessica Heesen (Hg.) *Handbuch Informations- und Medienethik*, Stuttgart: J.B. Metzler, 261–68.
- Baur-Ahrens, Andreas (2016): „‚Cyberwar' – Ein zentrales Problem der Sicherheitsdebatte?“, *Deutschland & Europa* 71, 58–62.
- Büttner, Barbara; Geminn, Christian L.; Hagendorff, Thilo; Lamla, Jörn; Ledder, Simon; Ochs, Carsten; Pittroff, Fabian (2016): Die Reterritorialisierung des Digitalen. Zur Reaktion nationaler Demokratie auf die Krise der Privatheit nach Snowden. Kassel: kassel university ppress.
- Hagendorff, Thilo (2017): Rassistische Maschinen? Übertragungsprozesse von Wertorientierungen zwischen Gesellschaft und Technik. In: Matthias Rath (Hg.): Brauchen Maschinen Ethik - und wenn ja, welche? Interdisziplinäre Perspektive auf selbständig "handelnde" und "kommunizierende" Systeme. Wiesbaden: Springer VS. (im Erscheinen)
- Hagendorff, Thilo (2017): Intimität und der Verlust der Informationskontrolle. In: Marlis Prinzing, Roger Blum, Mark Eisenegger und Patrik Ettinger (Hg.): Intimisierung des Öffentlichen. Wiesbaden: Springer VS. (im Erscheinen)
- Hagendorff, Thilo (2017): Resilienz und Mediennutzungsstrategien angesichts des digitalen Kontrollverlusts. In: Pamela Steen und Frank Liedtke (Hrsg.): Diskurs der Daten. Qualitative Zugänge zu einem quantitativen Phänomen. (im Erscheinen)
- Hagendorff, Thilo (2016): Open Data. In: Jessica Heesen (Hg.): Handbuch Informations- und Medienethik. Stuttgart: Metzler. S. 227–232.
- Hagendorff, Thilo (2016): Vertrauen und Solidarität im Kontext digitaler Medien. In: Petra Werner, Lars Rinsdorf, Thomas Pleil und Klaus-Dieter Altmeppen (Hg.): Verantwortung - Gerechtigkeit - Öffentlichkeit. Normative Perspektiven auf Kommunikation. Konstanz: UVK, S. 297–306.
- Hagendorff, Thilo (2017): Das Ende der Informationskontrolle. Digitale Mediennutzung jenseits von Privatheit und Datenschutz. Bielefeld: Transcript.

Vorträge und Präsentationen:

- Baur-Ahrens, Andreas, „The Power of Cyberspace Centralisation“, *9th Pan-European Conference on International Relations*, Giardini Naxos, 23.–26. September 2015
- Baur-Ahrens, Andreas, „An Ethical Perspective on the Power of Smart Devices“, *Smart Technologies – Workshop on Challenges and Trends for Privacy in a Hyper-connected World, IFIP Summer School 2015*, Edinburgh, 16.–21. August 2015
- Hagendorff, Thilo, Intimität und der Verlust der Informationskontrolle, Vortrag beim „Mediensymposium 2016 – Intimisierung des Öffentlichen“ (Luzern), Dezember 2016
- Hagendorff, Thilo, Anormalisierung und Selbstbestimmung - Handlungspsychologische Aspekte von Überwachung neu gedacht, Vortrag beim

III. Interdisziplinären Workshop "Privacy, Datenschutz & Surveillance" am Alexander von Humboldt Institut für Internet und Gesellschaft (Berlin), Dezember 2016

- Hagendorff, Thilo, Rassistische Maschinen?, Vortrag bei der Konferenz „Brauchen Maschinen Ethik – und wenn ja, welche? Interdisziplinäre Perspektiven auf selbständig ‚handelnde' und ‚kommunizierende' Systeme" (Ludwigsburg), Dezember 2016
- Hagendorff, Thilo, #GemeinsamEinsam – Wie verändern soziale Medien unser Zusammenleben?, Podiumsdiskussion zusammen mit Sonja Utz und Jochen Robes bei der Katholischen Hochschulgemeinde Tübingen (Tübingen), November 2016
- Hagendorff, Thilo, Social Media - Zwischen Privatheit, Kollektivität, Vernetzung und Entäußerung, Seminar bei der Ferienakademie des Cusanuswerks „Alles unter Kontrolle. Datenschutz und Selbstbestimmung in der digitalen Welt" (Niederalteich), August 2016
- Hagendorff, Thilo, Macht Google auch selig? Über die Herrschaft der Internetkonzerne und die Entfaltung gesellschaftlicher Gegenmacht (zusammen mit Dirk Helbing), Seminar bei der Wittenberger Sommerakademie „Gehirn, Gesellschaft, Gott und Google" (Lutherstadt Wittenberg), August 2016
- Hagendorff, Thilo, Informationskontrolle und smarte Technologien, Vortrag bei der Konferenz „Smart New World - Was ist ‚smart' an smarten Technologien?" am Institut für Technikfolgen-Abschätzung der Österreichischen Akademie der Wissenschaften (Wien), Mai 2016
- Hagendorff, Thilo, Privatsphäre im Umbruch – eine philosophische Anfrage, Vortrag bei der Tagung „Der Gläserne Mensch?" (Kloster Banz), Mai 2016
- Hagendorff, Thilo, Ethik der Open Data, Vortrag beim Praxis-Forum „Open Data" (Heidelberg), April 2016
- Hagendorff, Thilo, Überlegungen zum Ende der Informationskontrolle, Vortrag bei der Jahrestagung der Schweizerischen Gesellschaft für Kommunikations- und Medienwissenschaft (Fribourg), April 2016
- Hagendorff, Thilo, Datenkontrolle in der Datengesellschaft, Vortrag bei der Tagung „Daten\Gesellschaft!?" der Lehrstühle Technik- und Organisationssoziologie sowie Soziologie mit Schwerpunkt Gender und Technik (Aachen), März 2016
- Hagendorff, Thilo, Resilienz und Mediennutzungsstrategien angesichts des informationellen Kontrollverlusts, Vortrag bei der Konferenz „Diskurs der Daten" (Leipzig), Februar 2016
- Hagendorff, Thilo, Mediennutzungsstrategien für den informationellen Kontrollverlust, Vortrag beim Interdisziplinären Workshop „Privacy, Datenschutz & Surveillance" am Alexander von Humboldt Institut für Internet und Gesellschaft (Berlin), Dezember 2015
- Hagendorff, Thilo, Big Data - Was verbirgt sich hinter dem Begriff? Technische, ethische und sozialwissenschaftliche Fragestellungen, Vortrag beim Seminar „Führen in Zeiten wachsender Komplexität" am Fortbildungsinstitut der bayrischen Polizei (Ainring), November 2015
- Hagendorff, Thilo, Anonymität im Internet, Vortrag auf der Konferenz „Digitale Ethik 4.0" (Köln), Juni 2015
- Hagendorff, Thilo, Vertrauen ins Netz, Panelbeitrag auf der 60. Jahrestagung der Deutschen Gesellschaft für Publizistik- und Kommunikationswissenschaft (Darmstadt), Mai 2015

- Hagendorff, Thilo, Privatsphäre im Umbruch – eine philosophische Anfrage, Vortrag bei der Tagung „Der Gläserne Mensch?“ (Wildbad Kreuth), Mai 2015
- Hagendorff, Thilo, Medienethik, Workshop beim Deutschen Jungforschernetzwerk (Tübingen), Dezember 2014

Berichtsblatt

1. ISBN oder ISSN	2. Berichtsart (Schlussbericht oder Veröffentlichung) Schlussbericht
3. Titel Kartografie und Analyse der Privacy-Arena	
4. Autor(en) [Name(n), Vorname(n)] Ammicht Quinn, Regina Heesen, Jessica Baur-Ahrens, Andreas Hagendorff, Thilo Ledder, Simon Krautter, Jutta Pawelec, Maria	5. Abschlussdatum des Vorhabens 31.12.2016 6. Veröffentlichungsdatum Juni 2017 7. Form der Publikation Bericht
8. Durchführende Institution(en) (Name, Adresse) Internationales Zentrum für Ethik in den Wissenschaften (IZEW) Eberhard-Karls-Universität Tübingen Wilhelmstraße 19 72074 Tübingen	9. Ber. Nr. Durchführende Institution Projektkonto 3042002701 10. Förderkennzeichen 16KIS0097 11. Seitenzahl 34
12. Fördernde Institution (Name, Adresse) Bundesministerium für Bildung und Forschung (BMBF) 53170 Bonn	13. Literaturangaben 14. Tabellen 15. Abbildungen
16. Zusätzliche Angaben keine	
17. Vorgelegt bei (Titel, Ort, Datum)	
18. Kurzfassung Gegenwärtig gibt es, ausgelöst durch ein breites gesellschaftliches Problembewusstsein, zahlreiche politische Auseinandersetzungen, in denen Fragen nach dem ethischen und rechtlichen Stellenwert von Privatheit verhandelt werden. Dies ist insbesondere der Verbreitung informationstechnischer Systeme geschuldet. Im Kontext dieser Systeme kann Privatheit definiert werden über die Kontrolle, die eine Person darüber ausübt, wer Zugriff auf persönlichkeitsrelevante Daten und Informationen hat. Die Frage ist aber, wie weit diese Kontrolle überhaupt noch reicht, bedenkt man etwa die datenschutzrechtlich fraglichen Praktiken von Google, Facebook und ähnlichen Diensten. Je mehr persönlichkeitsrelevante Informationen zur elektronisch tauschbaren, wirtschaftlich verwertbaren Ressource werden, desto mehr werden etablierte Beschränkungen zur Verbreitung und Weitergabe von Informationen aufgelöst. Für Wirtschaftsunternehmen sind gerade personenbezogene Daten von großem Wert, schließlich erlaubt der Besitz dieser Daten, dass zielgenaue Kaufanreize beispielsweise über personalisierte Onlinewerbung gesetzt werden können. Aus dem Zusammenspiel wirtschaftlicher, polizeilicher, geheimdienstlicher, staatlicher wie auch persönlicher Interessen an personenbezogenen Daten sowie den Möglichkeiten informationstechnischer Systeme entsteht eine Dynamik, welche einerseits die Auflösung eines etablierten Verständnisses von Privatsphäre vorantreibt, aber andererseits neue Begriffe des Privaten sowie vielfältige Praxen der Grenzziehung zwischen Privatheit und Öffentlichkeit hervorbringt.	
19. Schlagwörter Privatheit, Datenschutz, Kartografie, digitale Technologie	
20. Verlag	21. Preis -

Document Control Sheet

1. ISBN or ISSN	2. type of document (e.g. report, publication) report
3. title Kartografie und Analyse der Privacy-Arena	
4. author(s) (family name, first name(s)) Ammicht Quinn, Regina Heesen, Jessica Baur-Ahrens, Andreas Hagendorff, Thilo Ledder, Simon, Krautter, Jutta Pawelec, Maria	5. end of project 31.12.2016 6. publication date June 2017 7. form of publication report
8. performing organization(s) (name, address) University of Tübingen International Centre of Ethics in the Sciences and Humanities (IZEW) Wilhelmstraße 19 72074 Tübingen	9. originator's report no. project account 3042002701 10. reference no. 16KIS0097 11. no. of pages 34
12. sponsoring agency (name, address) Bundesministerium für Bildung und Forschung (BMBF) 53170 Bonn	13. no. of references 14. no. of tables 15. no. of figures
16. supplementary notes	
17. presented at (title, place, date)	
18. abstract Caused by a broad societal awareness of problems, there are currently several political conflicts, debating the ethical and legal status of privacy. These debates take place especially due to the dissemination of information technology. In the context of this technology, privacy can be defined with regard to the control one has over the access of third parties to personal data and information. But the crucial question is how effective this control can be, considering for example the violation of data protection laws committed by Google, Facebook, and others. The more personal information becomes an electronically exchangeable, economically exploitable commodity, the more established constraints concerning the dissemination and transfer of information are dissolved. Especially personal data are of great value to companies, since the possession of these data allows targeted incentives, for example via personalized online advertising. The interplay of economic, police, intelligence, state as well as personal interests in personal data together with the possibilities of information technology creates a particular dynamic. On the one hand, this dynamic advances the dissolution of an established understanding of privacy. On the other hand, it creates new concepts of privacy and a variety of practices of demarcation between private and public.	
19. keywords privacy, data protection, mapping, digital technology	
20. publisher	21. price

Berichtsblatt

1. ISBN oder ISSN 978-3-7376-0306-5	2. Berichtsart (Schlussbericht oder Veröffentlichung) Veröffentlichung
3. Titel Privacy-Arena: Kontroversen um Privatheit im digitalen Zeitalter	
4. Autor(en) [Name(n), Vorname(n)] Baur-Ahrens, Andreas Hagendorff, Thilo Pawelec, Maria - Büttner, Barbara Lamla, Jörn (Hg.) Pittroff, Fabian - Barlag, Charlotte Geminn, Christian Miedzianowski, Nadine - Baumann, Joel (Hg.) Huntemann, Mike Paehr, Isabel Röder, Jörn	5. Abschlussdatum des Vorhabens 31.12.2016 6. Veröffentlichungsdatum Juni 2017 7. Form der Publikation Broschüre
8. Durchführende Institution(en) (Name, Adresse) Eberhard-Karls-Universität Tübingen Internationales Zentrum für Ethik in den Wissenschaften (IZEW) Wilhelmstraße 19 72074 Tübingen - Universität Kassel Fachbereich Soziologische Theorie Nora-Platiel-Straße 5 34109 Kassel - Universität Kassel Fachgebiet Öffentliches Recht Pfannkuchstraße 1 34109 Kassel - Kunsthochschule Kassel Menzelstraße 13 34121 Kassel	9. Ber. Nr. Durchführende Institution Projektkonto 3042002701 10. Förderkennzeichen 16KIS0097 11. Seitenzahl 196
12. Fördernde Institution (Name, Adresse) Bundesministerium für Bildung und Forschung (BMBF) 53170 Bonn	13. Literaturangaben 14. Tabellen 15. Abbildungen
16. Zusätzliche Angaben keine	
17. Vorgelegt bei (Titel, Ort, Datum) Forum Privatheit: Symposium "Von Profiling bis Fake News", Berlin, 22. Juni 2017	

18. Kurzfassung
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.

19. Schlagwörter
Privatheit, Datenschutz, Kartografie, digitale Technologie

20. Verlag	21. Preis
kassel university press	open access/ 29,90€ für Druckausgabe

Document Control Sheet

1. ISBN or ISSN 978-3-7376-0306-5	2. type of document (e.g. report, publication) publication
3. title Privacy-Arena: Kontroversen um Privatheit im digitalen Zeitalter	
4. author(s) (family name, first name(s)) Baur-Ahrens, Andreas Hagendorff, Thilo Pawelec, Maria - Büttner, Barbara Lamla, Jörn (ed.) Pittroff, Fabian - Barlag, Charlotte Geminn, Christian Miedzianowski, Nadine - Baumann, Joel (ed.) Huntemann, Mike Paehr, Isabel Röder, Jörn	5. end of project 31.12.2016 6. publication date June 2017 7. form of publication Broshure
8. performing organization(s) (name, address) University of Tübingen International Centre of Ethics in the Sciences and Humanities (IZEW) Wilhelmstraße 19 72074 Tübingen - University of Kassel Department of Sociology Nora-Platiel-Straße 5 34109 Kassel - University of Kassel Department of Public Law Pfannkuchstraße 1 34109 Kassel - Kunsthochschule Kassel Menzelstraße 13 34121 Kassel	9. originator's report no. project account 3042002701 10. reference no. 16KIS0097 11. no. of pages 196
12. sponsoring agency (name, address) Bundesministerium für Bildung und Forschung (BMBF) 53170 Bonn	13. no. of references 14. no. of tables 15. no. of figures
16. supplementary notes	
17. presented at (title, place, date) Forum Privatheit: Symposium "Von Profiling bis Fake News", Berlin, 22 June 2017	

18. abstract

In times of digitalisation and networking, privacy remains a controversial and disputed issue. Not only do states gain access to new forms of surveillance; new and evolving business models on the market increasingly challenge traditional notions of privacy. Instead of attempting to pin down a definition of this realignment, it rather seems beneficial to engage with the many different issues concerning the future of privacy. The research project 'Mapping and Analysis of the privacy arena', funded by the German Federal Ministry of Education and Research, follows this approach. Following perspectives from sociology, law, ethics and visual communication, this research deals with several conflicts of interpretations of privacy as well as the ethical and legal significance of the concept.

Addressed issues include political moments of new technologies such as cryptography, democratic strategies towards dealing with governmental surveillance within the NSA investigation committee in the German parliament (Bundestag), vast consequences of algorithmic productions of reality through big data as well as conflicting interests concerning the passing of the EU General Data Protection Regulation. Furthermore, this research approach includes perspectives of Science and Technology Studies, actor-network-theory, mapping-procedures by Adele Clarke as well as the theories of social worlds and arenas by Anselm Strauss. This volume has been supplemented by a recent exhibition on privacy in Kassel (December 2016) and the webpage privacy-arena.net.

19. keywords

privacy, data protection, mapping, digital technology

20. publisher	21. price
kassel university press	open access/ 29.00 € for hard copy