forum <privatheit>
selbstbestimmtes_leben_in_der_digitalen_welt

FORUM PRIVATHEIT UND SELBSTBESTIMMTES LEBEN IN DER DIGITALEN WELT

Policy Paper

DATENSCHUTZ STÄRKEN, INNOVATIONEN ERMÖGLICHEN

Wie man den Koalitionsvertrag ausgestalten sollte

IMPRESSUM

Autoren:
Alexander Roßnagel[1], Tamer Bile[1], Christian Geminn[1], Olga Grigorjew[1], Paul C. Johannes[1], Murat Karaboga[2], Nicole Krämer[3], Natalie Maier[1], Nicholas Martin[2], Johannes Müller[1], Maxi Nebel[1], Michael Friedewald[2], Benjamin Bremert[4]

(1) Universität Kassel, Projektgruppe verfassungsverträgliche Technikgestaltung im Wissenschaftlichen Zentrum für Informationstechnik-Gestaltung (ITeG)
(2) Fraunhofer-Institut für System- und Innovationsforschung ISI, Karlsruhe
(3) Universität Duisburg-Essen, Fachgebiet Sozialpsychologie: Medien und Kommunikation
(4) Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein

Die Ansichten, die in diesem Bericht wiedergegeben werden, sind die der Verfasser und nicht notwendigerweise die offizielle Meinung ihrer Institutionen oder der anderen Projektpartner.

Kontakt:
Michael Friedewald

Telefon +49 721 6809-146
Fax +49 721 6809-315
E-Mail info@forum-privatheit.de

Fraunhofer-Institut für System- und Innovationsforschung ISI
Breslauer Straße 48
76139 Karlsruhe

www.isi.fraunhofer.de
www.forum-privatheit.de

Schriftenreihe:
Forum Privatheit und selbstbestimmtes Leben in der digitalen Welt
ISSN-Print 2199-8906
ISSN-Internet 2199-8914

1. Auflage, März 2018

Digitalisierung, Privatheit und Selbstbestimmung

Der Koalitionsvertrag zwischen CDU, CSU und SPD verspricht einen „neuen Aufbruch für Europa", eine „neue Dynamik für Deutschland" und einen „neuen Zusammenhalt für unser Land". Diesem Titel ihres Vertrags entsprechend wollen die Koalitionäre umfangreiche Modernisierungen anstoßen. Sie formulieren damit einen Gestaltungsanspruch, der sich vor allem auch auf die Digitalisierung von Wirtschaft und Gesellschaft bezieht. Digitalisierung verändert gesellschaftliche Infrastrukturen und bringt neue hervor. Sie erzeugt neue oder modifiziert bekannte individuelle und kollektive Verhaltensweisen. Sie beeinflusst damit tiefgreifend die Verwirklichungsbedingungen von Privatheit und Selbstbestimmung. Wer angesichts der Intensität und Dynamik der Veränderungen nicht passives Objekt der Digitalisierung werden will, muss sie gestalten. Dies wird im Koalitionsvertrag in Aussicht gestellt, erfordert für eine erfolgreiche Umsetzung jedoch konsequente Anstrengungen.

Risiken minimieren, Chancen nutzen

Jede Gestaltung der Digitalisierung muss zwei Ziele verfolgen: ihre Risiken mindern und ihre Chancen nutzen. Beides kann zu Innovationen führen. Politische Maßnahmen, die nur die Chancen im Blick haben, verfehlen die Aufgabe der umfassenden und verantwortlichen politischen Gestaltung. Diese Aufgabe formuliert auch der Koalitionsvertrag der Bundesregierung für die laufende Legislaturperiode (2017-21). Als politische Grundlage der Großen Koalition ist der Koalitionsvertrag ein Kompromiss, der nur das konkret benennt, worauf sich die Koalitionäre inhaltlich einigen konnten. Vieles wird, weil noch keine wirkliche Einigung erzielt worden ist, nur angedeutet, bleibt im Ungefähren oder erfährt nur eine abstrakte Formulierung.

Der Expertenkreis „Forum Privatheit und selbstbestimmtes Leben in der digitalen Welt" hat den Koalitionsvertrag daraufhin analysiert, welche Aussagen er zur Gestaltung der Digitalisierung mit Blick auf wirtschaftliche und soziale Innovationen sowie Privatheit und Selbstbestimmung enthält. Für diese untersucht das Policy Paper in konstruktiver Absicht, mit welchen Maßnahmen die Aussagen im Koalitionsvertrag in der kommenden Legislaturperiode unterlegt werden müssten, um die Bedingungen für beide Zielsetzungen zu verbessern.

Die folgende Kurzanalyse orientiert sich an unterschiedlichen Handlungsmöglichkeiten der künftigen Bundesregierung. Sie stellt im Kapitel „Innovationen und Datenschutz in der Europäischen Union" Maßnahmen vor, die Deutschland in dem durch Unionsvorgaben strukturierten Feld selbst umsetzen oder in die Diskussion in der Union einbringen kann.

Das Kapitel „Innovationen und Datenschutz in Deutschland" beschreibt Maßnahmen, die demokratische Politik in Deutschland ohne Beschränkungen durch die Union ergreifen kann.

Das Kapitel „Digitalisierung und Selbstbestimmung" wendet sich Rahmenbedingungen zu, die nicht unmittelbar Privatheit und Selbstbestimmung betreffen, aber auf ihre Verwirklichungsbedingungen großen Einfluss haben.

Innovationen und Datenschutz in der Europäischen Union

„Daten sind der Treibstoff für Innovationen und neue Dienste. Diese wollen wir ermöglichen und gleichzeitig den hohen und weltweit angesehenen Datenschutzstandard Europas und Deutschlands halten“ (2069f.).[1]

Datengetriebene Innovationen

Verglichen mit früheren Koalitionsverträgen sieht der aktuelle Vertrag Datenschutz als ein wichtiges Thema an, auch um datengetriebene Innovationen zu ermöglichen. Die Koalition spielt gerade nicht Innovationsbedarf gegen Datenschutz aus, sondern erkennt, dass sich beide gegenseitig bedingen. Datenschutz benötigt in einer sich durch Digitalisierung rasant ändernden Welt Innovationen, um Privatheit und Selbstbestimmung gewährleisten zu können. Umgekehrt benötigen Innovationen Datenschutz, um Anreize zu erhalten, um Alleinstellungsmerkmale zu etablieren und um das Vertrauen bei denjenigen zu gewinnen, die Innovationen annehmen und nutzen sollen.

Datenschutz als Faktor im Wettbewerb

Die Koalition folgt zu Recht nicht der verbreiteten Annahme, dass hoher Datenschutz Innovation und Wirtschaftsentwicklung hemmt. Diese These ist, auch wenn sie oft medienwirksam geäußert wird, wissenschaftlich kaum untersucht. Zwar trifft es zu, dass sehr hohe regulatorische Auflagen Wettbewerbsfähigkeit schmälern und Innovation verhindern *können*. Es gibt allerdings kaum belastbare Erkenntnisse, ob dieser Zustand im Datenschutz erreicht ist. Wie die Innovationsforschung hinreichend belegt hat, ist der Glaube, hohe Standards führten zwangsläufig zu einer Absenkung der Wettbewerbsfähigkeit und bremsten Anreize für Innovation aus, unzutreffend. Im Gegenteil können hohe Auflagen Innovation begünstigen (sie erfordern Lösungen) und Anreize für Unternehmen setzen, sich am Markt eher über Produktqualität als über niedrige Preise zu differenzieren – was wiederum innovationssteigernd wirkt und dadurch Wettbewerbsfähigkeit mittelfristig eher fördert.

Erhalt hoher Standards im Datenschutz

Wenn die Koalition datengetriebene Innovationen ermöglichen und gleichzeitig den hohen Datenschutzstandard Europas und Deutschlands halten will, kann sie nicht Geschäftsmodelle fördern und dabei deren Risiken für Privatheit und informationelle Selbstbestimmung der betroffenen Personen außer Acht lassen. Daher beabsichtigt sie, parallel zur Förderung von innovativen Datenverarbeitungsmodellen einen Rechtsrahmen zu konzipieren, um diesen Risiken wirksam begegnen zu können.

Weiterentwicklung der Datenschutz-Grundverordnung

Die Koalition will die Mitte 2020 anstehende Evaluierung der Datenschutz-Grundverordnung durch die EU-Kommission intensiv begleiten und dabei alle Regelungen auf ihre „Zukunftsfähigkeit und Effektivität“ hin überprüfen (2082ff., 6109ff.). Zukunftsfähigkeit und Effektivität sind geeignete Kriterien, um die Datenschutz-Grundverordnung weiterzuentwickeln. Hinsichtlich beider Kriterien hat sie Defizite. Zukunftsfähigkeit fehlt ihr insofern, als sie risikoneutral keine der absehbaren Herausforderungen – wie etwa Big Data, künstliche Intelligenz, selbstlernende Systeme, Suchmaschinen, Netzwerkplattformen, Kontexterfassung, Internet der Dinge – adressiert. Will sie zukunftsfähig

[1] Die Zahlen in Klammern bezeichnen die Zeilennummern der Zitate in der Fassung vom 7.2.2018, https://www.cdu.de/system/tdf/media/dokumente/koalitionsvertrag_2018.pdf?file=1 und https://www.spd.de/fileadmin/Dokumente/Koalitionsvertrag/Koalitionsvertrag_2018.pdf.

sein, muss sie gerade die enormen Risiken, die von der Digitalisierung aller Lebensbereiche ausgehen und die durch die zentralen Infrastrukturen der digitalen Gesellschaft verursacht werden, gezielt aufgreifen. Technik- und damit auch risikoneutrale allgemeine und hochabstrakte Regelungen genügen dafür nicht. Sie gefährden vielmehr Innovationen, weil sie durch ihre vielfältige Auslegungsfähigkeit keine Rechtssicherheit für Investoren bieten. Diese Risikoneutralität gefährdet auch die Effektivität der Regelungen. Nur wenn sie die Vermeidung oder Minderung der Risiken in einer ihnen adäquaten Weise regeln, sind sie vollziehbar und reduzieren auch die von digitalen Anwendungen ausgehendend Risiken. Erst so sind sie für Hersteller und Anbieter, Aufsichtsbehörde und betroffene Person klar, eindeutig, nachvollziehbar und umsetzbar.[1]

Einrichtung eines Innovationsboards

Die Koalition strebt an, ein „Innovationsboard auf EU-Ebene" einzurichten, das „Vorschläge zur Weiterentwicklung der Europäischen Datenschutzregelungen" erarbeitet (2082ff.). Die Wechselwirkungen von Datenschutz und Innovationstätigkeit zu erforschen kann hilfreich sein, wenn das Board richtig zusammengesetzt ist. Sollten bestimmte Regeln Schlüsseltechnologien tatsächlich ausbremsen, wäre eine Debatte über Nachjustierungen angemessen, soweit Grundrechte nicht beeinträchtigt werden. Das Board darf keinesfalls so besetzt werden, dass in ihm diejenigen überwiegen, die etablierte Industrien vertreten und sich einseitig für die Aufweichung des Datenschutzes einsetzen. Gerade wegen der hohen Unsicherheit, ob und wie Datenschutzregeln Innovation beeinflussen, ist es essentiell, dass ein solches Board wissenschaftlich-objektiv und nicht lobbygeleitet arbeitet und auch das zivilgesellschaftliche Interesse an sozialer Innovation berücksichtigt. Dies wäre auch im Sinn echter Innovationsförderung, die kein Bestandsschutz sein darf: Innovatoren liegen per Definition im Wettbewerb mit etablierten wirtschaftlichen Interessen, sind aber, was Lobby-Macht angeht, strukturell schwächer aufgestellt als diese. Ein von den etablierten Industrien dominiertes Board könnte nicht nur als Datenschutz-, sondern auch Innovationshemmnis wirken.

Innovatives Einwilligungsmanagement

Zudem macht sich die Koalition für eine innovationsfreundliche Anwendung der Datenschutz-Grundverordnung stark und will die Datenportabilität und die Interoperabilität von Plattformen sowie „die Rechte der Nutzer stärken" (2091ff.). Hierzu will sie die Entwicklung von „innovativem Einwilligungsmanagement" fördern und unterstützen sowie sich für eine „Stärkung der Kompetenz der Nutzerinnen und Nutzer", für „mehr Transparenz" und „Privacy by Default" und „Privacy by Design" (d.h., datenschutzfreundliche Voreinstellungen und Systemgestaltung) „auf Seiten der Anbieter" einsetzen (2086ff.). Auch verspricht sie die Förderung einer sicheren, mobilen, digitalen Identifizierung und Authentifizierung unter benutzerfreundlichem Einsatz des elektronischen Personalausweises (1984ff., 2040ff., 6102) mit Opt-in-Lösung für die Nutzenden. „Ende-zu-Ende-Verschlüsselung" soll „für jedermann verfügbar" sein (1985ff.).

Verbrauchervertrauen

Zu Recht erkennt die Koalition, dass fehlendes Nutzer- und Verbrauchervertrauen die Entwicklung der Digitalökonomie hemmt. Wenn Verbraucherinnen und Verbraucher Vertrauen in die Sicherheit ihrer Daten fehlt (etwa, weil sie vermuten, dass Anbieter den Schleier unverständlicher AGBs ausnutzen, um ihre Daten für alle möglichen Zwecke weiterzuverwenden), dann werden sie die angebotenen Dienste im Zweifel nicht nutzen, mit entsprechendem Schaden für die europäische Digitalökonomie. Empirische Untersuchungen belegen immer wieder, dass Verbraucher und Verbraucherinnen meist nur wenig Vertrauen in die Datenschutzstandards digitaler Unternehmen haben und dieses Vertrauen weiter abnimmt. Transparente AGBs, die den Nutzerinnen und Nutzern ein klares Verständnis der geplanten Datenverarbeitungen bieten und ein innova-

[1] S. hierzu das Forum Privatheit Policy Paper „Die neue Datenschutz-Grundverordnung", 2016.

tives Einwilligungsmanagement, das mehr Kontrolle über die Nutzerdaten ermöglicht, sowie Datenschutz durch Systemgestaltung und Voreinstellungen, einfache und sichere Authentifizierung und Vertraulichkeitsschutz durch Ende-zu-Ende-Verschlüsselung können Verbrauchervertrauen und dadurch Europa als Innovationsstandort stärken. Zu Recht sieht die Koalition Datenschutz und Nutzerrechte als Grundlage und Bedingung für nützliche Innovationen und Wirtschaftsförderung.

Unterstützung für Start-ups

Die Koalition will außerdem erreichen, „dass z. B. Start-ups und Unternehmen bei digitalen Innovationen einen beratenden Ansprechpartner für Datenschutzfragen erhalten und deutschlandweit geltende Entscheidungen einholen können" (2079ff). Die Last und die Mehrkosten, die rechtliche Vorschriften Unternehmen aufbürden, hängen ganz erheblich von der Komplexität und Rechtssicherheit dieser Regelungen ab. Insbesondere die Regelungen der europäischen Datenschutzreform haben zusammen mit den deutschen Umsetzungsgesetzen die Komplexität der Vorgaben erheblich erhöht und die Rechtssicherheit deutlich verringert. Die Idee, gerade jungen Unternehmen Möglichkeiten schneller und verlässlicher Beratung anzubieten, ist daher naheliegend. Allerdings sind für ihre Umsetzung grundlegende rechtliche und verwaltungstechnische Vorgaben zu beachten. Die Aufsichtsbehörden des Bundes und der Länder haben in ihren Zuständigkeitsbereichen bereits durch die Datenschutz-Grundverordnung den Auftrag, verantwortliche Datenverarbeiter in Datenschutzfragen zu beraten. Sie sind auch diejenigen Stellen, die in voller Unabhängigkeit die Umsetzung der datenschutzrechtlichen Vorgaben überwachen und diese für den praktischen Vollzug auslegen. Sie müssten für eine solche – mit massivem Mehraufwand verbundene – Aufgabe aber entsprechend finanziell und personell ausgestattet werden. Diese können auch für ihren Zuständigkeitsbereich deutschlandweit geltende Entscheidungen treffen. Sie müssen sich jedoch in allen wichtigen Fragen mit den anderen deutschen Aufsichtsbehörden abstimmen und die Entscheidung des Europäischen Datenschutzausschusses einholen. Deutschlandweite oder unionsweite Entscheidungen wird es nur nach Durchlaufen dieser Verfahren geben. Durch die Vorgaben der Datenschutz-Grundverordnung hat der deutsche Gesetzgeber keine Möglichkeit, innovationsfreundlichere Verfahren festzulegen.

Plattformunternehmen

Schließlich verfolgt die Koalition das Ziel, starke deutsche und europäische Plattform-Unternehmen zu schaffen. Einschlägige Hemmnisse sollen abgebaut werden. Ein „level playing field", zu dem auch „die Rechte von Beschäftigten und Verbrauchern" gehören, soll entstehen. Dazu will die Koalition „die Mitwirkung der Plattformen einfordern" (1951ff.). In diesem Zusammenhang soll auch das Wettbewerbsrecht überarbeitet werden (2776ff.). Zutreffend erkennt sie, dass in der Plattformökonomie oft starke Netzwerkeffekte mit entsprechender Monopolbildung vorherrschen: Es gewinnt nicht das beste oder billigste Produkt, sondern jenes, das am schnellsten eine marktbeherrschende Stellung aufbaut, z. B. aufgrund zufälliger First-Mover-Vorteile. Nachzügler mit besseren (z. B. datenschutzfreundlicheren) Angeboten bleiben dann aufgrund der Netzwerkeffekte außen vor. Datenportabilität und Interoperabilität der Plattformen sowie die Modernisierung des Wettbewerbsrechts sollen helfen, diese Effekte zu minimieren. Auch in diesem Zusammenhang sind Datenschutz und Nutzerrechte wettbewerbs- und innovationsfördernde Mittel. Dies ist sowohl aus datenschutz- als auch aus innovationspolitischer Perspektive zu begrüßen. Entscheidend wird letztlich die Durchsetzung dieser Anforderungen gegenüber weltweit agierenden Plattformanbietern sein.

Da die Datenschutz-Grundverordnung keine vollständige Harmonisierung des Datenschutzrechts in der Union bewirkt, sondern zu einer Ko-Regulierung mit den Mitgliedstaaten führt, hängt Zukunftsfähigkeit und Effektivität der Datenschutzregelungen vor allem von den Mitgliedstaaten ab.[1] Um die genannten Ziele zu erreichen, muss die Koalition daher prüfen, ob Deutschland entsprechende datenschutzfördernde Regelungen erlassen kann. Die Bundesregierung hat in der letzten Legislaturperiode nur in einem sehr geringen Umfang von den Öffnungsklauseln in der Datenschutz-Grundverordnung Gebrauch gemacht. Dies ist jedoch unabdingbar für die Weiterentwicklung des Datenschutzrechts. Die Bundesregierung sollte deshalb die in der Datenschutz-Grundverordnung enthaltenen Regelungsoptionen dazu nutzen, das europäische Datenschutzrecht weiterzuentwickeln und zu modernisieren, um auf diese Weise für die Datenschutzreform in der Union Vorbild zu sein.

Ko-Regulierung zwischen EU und Mitgliedstaaten

E-Privacy-Verordnung

Auch bei der geplanten E-Privacy-Verordnung verfolgt die Koalition das zusammenhängende Doppelziel, ein „hohes Schutzniveau für die Vertraulichkeit von Kommunikationsdaten" zu gewährleisten „und zugleich den Spielraum für Innovationen und digitale Geschäftsmodelle" zu erhalten (2077ff.). Um die Grundrechte zu stärken und die Wettbewerbssituation deutscher und europäischer Anbieter zu stärken, sollte die Bundesregierung in der Entschließung des Rats und in den folgenden Trilog-Verhandlungen die Forderung der Kommission und des Parlaments unterstützen, den Nutzerinnen und Nutzern mehr Kontrolle über ihre Daten zu geben. Nach diesen Vorschlägen soll die E-Privacy-Verordnung vorsehen, dass Unternehmen Daten ohne Einwilligung betroffener Personen nicht kommerziell verarbeiten dürfen. Die E-Privacy-Verordnung unterscheidet sich von der Datenschutz-Grundverordnung vor allem dadurch, dass sie ihre Vorgaben nicht radikal technikneutral formuliert und stattdessen risikospezifische und damit rechtssichere Regelungen vorsieht. Zwar wünschen Stimmen aus der Internet- und Telekommunikationswirtschaft eine Regelung der „Abwägung überwiegender betroffener Interessen" nach dem Modell der Datenschutz-Grundverordnung. Dieses Modell führt jedoch zu mangelnder Rechtssicherheit. Die Bundesregierung sollte sich daher nicht für eine Regelung einsetzen, die allein auf die Abwägung überwiegender berechtigter Interessen abstellt und Risiken und Folgen für die betroffenen Personen ignoriert. Ein Opt-in, so wie es die bisherigen Entwürfe zur E-Privacy-Verordnung vorsehen, ist eine adäquate Regelung, um zu effektivem und zukunftsorientiertem Schutz von Privatheit und informationeller Selbstbestimmung im Bereich elektronischer Kommunikation beizutragen.

Datentransfer in Drittstaaten

EU/US-Privacy-Shield

„Freier und sicherer Datenaustausch mit anderen Wirtschaftsräumen ist eine Grundvoraussetzung für den Erfolg der deutschen und europäischen Digitalwirtschaft." Daher will die Koalition den transatlantischen Datenaustausch auf Grundlage des EU/US-Privacy-Shield erhalten und zum Vorbild für den Datenaustausch auch mit anderen Weltregionen nehmen (1890ff.). Hierfür sind allerdings die Vorgaben des Europäischen Gerichtshofs zu beachten. Dieser hat die Entscheidung der Europäischen Kommission zum Safe Harbor-Abkommen mit der Begründung für ungültig erklärt, dass es in den Vereinigten Staaten keine wirksamen Mechanismen zur Begrenzung und Kontrolle der Massenüberwachung durch US-Geheimdienste gibt und für EU-Bürgerinnen und Bür-

[1] S. hierzu das Forum Privatheit Policy Paper „Nationale Implementierung der Datenschutz-Grundverordnung", 2018.

ger kein wirksamer Rechtsschutz gegen diese Überwachung besteht. Mit dem Nachfolgeabkommen zum EU/US-Privacy-Shield sollten diese Mängel behoben werden. Die europäischen Datenschutzbehörden und auch die Kommission haben jedoch festgestellt, dass die US-Seite die vom Europäische Gerichtshof bemängelten Defizite nur unzureichend behoben hat. Bevor die Bundesregierung sich auf dieses Abkommen verlässt und es sogar zum Vorbild erklärt, müsste sie erst einmal auf vollständige Erfüllung des Abkommens drängen und dessen Nachbesserung in einem Umfang erreichen, dass die vom Europäische Gerichtshof genannten Mängel vollständig behoben sind. Erst wenn die ernsthaften Bedenken aus dem Weg geräumt und der Grundrechtsschutz gewährleistet sind, könnte das Privacy-Shield-Abkommen tatsächlich als Vorbild für weitere Abkommen mit anderen Weltregionen dienen.

Europäische digitale Grundrechtecharta

Verbesserung der Verwirklichungsbedingungen bestehender Grundrechte

Für die Koalition sind „im digitalen Zeitalter … universelle Spielregeln wichtig". Dazu soll die Bundesregierung „das Projekt einer europäischen digitalen Grundrechtecharta" begleiten. Durch sie „sollen die Chancen und Risiken der Digitalisierung zu einem gerechten Ausgleich gebracht werden" (2229ff.). Das Ziel einer „digitalen Grundrechtecharta" ist jedoch bei näherer Betrachtung nicht zielführend. Die im Bereich des Datenschutzes maßgebliche Charta der Grundrechte der Europäischen Union bietet bereits einen umfassenden Schutz gegen die Gefahren der Digitalisierung. In Deutschland besteht das Recht auf informationelle Selbstbestimmung und auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme. Die Diskussion um neue Grundrechte darf nicht davon ablenken, bestehendes Rechts zu vollziehen.

Innovationen und Datenschutz in Deutschland

Das Datenschutzrecht der Union bietet nur Grundstrukturen und einen Rahmen für das geltende und das künftige Datenschutzrecht. In vielen Bereichen – insbesondere im Bereich öffentlicher Verwaltung – verbleibt den Mitgliedstaaten die Regelungskompetenz für den Datenschutz.[1] Diese will die Koalition auch nutzen. Vorschläge, wie diese Absicht verwirklicht werden kann, bietet das folgende Kapitel.

Beschäftigtendatenschutz

Die Koalition erkennt, dass die Digitalisierung zahlreiche Vorteile für Unternehmen und Beschäftigte bietet, zugleich aber auch Überwachungs- und Kontrollpotentiale birgt und daher die Sorge vor dem „gläsernen Mitarbeiter" berechtigt ist. Daher will sie „Klarheit über Rechte und Pflichten der Arbeitgeberinnen und Arbeitgeber, der Arbeitnehmerinnen und Arbeitnehmer schaffen sowie die Persönlichkeitsrechte der Beschäftigten sicherstellen (Beschäftigtendatenschutz)" (1837ff., 6108).

Risikoadäquate Regelungen

Zu diesem Zweck sollte die Bundesregierung – wie bereits in der Gesetzesbegründung zu § 26 BDSG n.F. 2017 angesprochen – risikoadäquate besondere Datenschutzregelungen für das Beschäftigungsverhältnis treffen. Hierzu gehören u. a. Regelungen, die

[1] S. hierzu das Forum Privatheit Policy Paper „Nationale Implementierung der Datenschutz-Grundverordnung", 2018.

heimliche Kontrollen ebenso explizit ausschließen wie eine Dauerüberwachung und die Erstellung umfassender Bewegungsprofile. Ebenso sollte die Lokalisierung von Beschäftigten auf jene Fälle begrenzt werden, in denen sie tatsächlich betriebsbedingt erforderlich ist und auch in diesen Fällen zeitlich begrenzt sein. Zusätzlich sollten Arbeitgeber die Pflicht haben, die Architektur ihrer mobilen Datenverarbeitung dahingehend zu überprüfen, ob personenbezogene Daten der Beschäftigten in ihren Endgeräten verbleiben können und nur in anonymisierter oder pseudonymisierter Form auf zentralen Servern des Arbeitgebers verarbeitet werden. Da die bloße Übernahme der bisherigen Regelungen diesen Anforderungen nicht gerecht wird, sollte die Koalition bei ihren Regulierungsvorhaben betriebliche Realitäten und technische Möglichkeiten berücksichtigen und den Risiken der Technologien entsprechende Regelungen treffen.

E-Government

Die Koalition will „in einem digitalen Portal für Bürgerinnen und Bürger sowie für Unternehmen einen einfachen, sicheren und auch mobilen Zugang zu allen Verwaltungsdienstleistungen ermöglichen. Dazu vernetzen wir geeignete zentrale und dezentrale Verwaltungsportale in einem Portalverbund. In dem damit verknüpften Bürgerkonto hat der Bürger Einblick, welche Daten beim Staat vorliegen, welche Behörde darauf Zugriff genommen hat und kann den Umgang mit seinen persönlichen Daten steuern“ (2005ff.). Die Koalition will außerdem zügig „eine vollständig elektronische Vorgangsbearbeitung in der öffentlichen Verwaltung (E-Akte)“ einführen (2033). Weiterhin will sie mit Hilfe des elektronischen Personalausweises Behörden ermöglichen, Daten über gemeinsame Register und eindeutige, registerübergreifende Identifikationen zu verknüpfen („once only“-Prinzip) (2045, 6082ff.). Dabei will sie eine Opt-in-Lösung verankern, „die das Zustimmungsrecht der Bürgerinnen und Bürger festschreibt“ (2043).

Diese Maßnahmen können die Verarbeitung von Bürgerdaten für die Verwaltung, aber auch für die Bürgerinnen und Bürger erleichtern. Dabei ist jedoch darauf zu achten, dass die Selbstbestimmung der Bürgerinnen und Bürger und die Zweckbindung der Daten gewährleistet bleibt. Opt-in-Lösungen sind dafür der richtige Weg. Diese setzen eine ausreichende Transparenz über die Datenverarbeitung und ihre Zwecke voraus. Um Risiken für den Datenschutz und die Datensicherheit zu minimieren, müssen die Systeme unter Berücksichtigung der Grundsätze Datenschutz „by Design“ und „by Default“ sicher gestaltet werden. Verbindliche Konzepte für die Implementierung von Ende-zu-Ende-Verschlüsselung, Datenschutzgarantien und umfassendes Datenschutz- und Informationssicherheitsmanagement sind dafür essentiell. In der Aus- und Weiterbildung der Behördenmitarbeiterinnen und -mitarbeiter ist eine starke Sensibilisierung hinsichtlich Datenschutz und Informationssicherheit erforderlich.

Cybersicherheit

Einbindung aller relevanten Gruppen

Für ein grundlegendes Vertrauen in die Sicherheit und Vertraulichkeit von Kommunikation, Daten und IT-Strukturen verspricht die Koalition, in einem Nationalen Pakt Cybersicherheit alle gesellschaftlich relevanten Gruppen, Hersteller, Anbieter und Anwender sowie die öffentliche Verwaltung in gemeinsamer Verantwortung für digitale Sicherheit einzubinden, in einem Cyberbündnis mit der Wirtschaft bestehende Strukturen zu bündeln und die Zusammenarbeit von Staat und Wirtschaft auszubauen. Dazu soll das IT-Sicherheitsgesetz fortgeschrieben und der Ordnungsrahmen erweitert werden (1967ff., 5888ff.).

Ausbau des BSI zur nationalen Cybersicherheitsbehörde

Das BSI soll als nationale Cybersicherheitsbehörde ausgebaut und als Beratungsstelle für Fragen der IT-Sicherheit dienen, der Verbraucherschutz als zusätzliche Aufgabe des BSI etabliert und das BSI als zentrale Zertifizierungs- und Standardisierungsstelle für IT- und Cyber-Sicherheit gestärkt werden. Einfache und sichere Lösungen für die elektronische Identifizierung und Ende-zu-Ende-Verschlüsselung sollen für

jedermann ermöglichen, verschlüsselt mit der Verwaltung über gängige Standards zu kommunizieren (1984f.). Hersteller und Anbieter digitaler Produkte und Dienstleistungen sollen stärker in die Pflicht genommen, klare Regelungen für die Produkthaftung aufgestellt, „Security by Design" gefördert, Sicherheitsstandards für internetfähige Produkte entwickelt und deren Einhaltung mit einem Gütesiegel für IT-Sicherheit zertifiziert werden. Diese Maßnahmen stärken auch die Transparenz, Privatheit und Selbstbestimmung der Betroffenen und sind uneingeschränkt zu begrüßen.

Innere Sicherheit und Polizei

In Kapitel X „Ein handlungsfähiger und starker Staat für eine freie Gesellschaft" (5765 ff.) wird im Koalitionsvertrag ein „Pakt für den Rechtstaat" (5767) vorgestellt. Er strebt zum einen den personellen Ausbau und bessere finanzielle und technische Ausstattung der Sicherheitsbehörden des Bundes an (5786). Zum anderen ist der Ausbau von deren Befugnissen bei gleichzeitiger Erleichterung des Datenaustauschs zwischen den Behörden Schwerpunkt. So soll z. B. die molekulargenetische Untersuchung nach § 81e StPO nicht mehr nur auf die Feststellung der Abstammung und des Geschlechts beschränkt sein, sondern auch auf die Feststellung äußerlicher Merkmale wie Haar-, Augen- und Hautfarbe sowie des Alters und damit auch auf besondere Kategorien personenbezogener Daten ausgeweitet werden (5805). Ausgebaut und technisch verbessert werden soll die (intelligente) Videoüberwachung an öffentlichen Straßen und Plätzen (5964ff.). Der Koalitionsvertrag fordert weiter für Sicherheitsbehörden gleichwertige Befugnisse im Umgang mit dem Internet wie außerhalb des Internets (6023). Er strebt außerdem einheitliche Regelungen nach einem gemeinsamen Musterpolizeigesetz an, wie es bereits die Innenministerkonferenz beschlossen hat. Dieses sollte jedoch nicht nur erreichen, dass es „keine Zonen unterschiedlicher Sicherheit" gibt, sondern auch darauf hinwirken, dass die Geeignetheit, Erforderlichkeit und Angemessenheit aller Befugnisse und Maßnahmen kritisch überprüft wird. Außerdem will der Koalitionsvertrag das Bundeskriminalamt als zentrales Datenhaus im polizeilichen Informationsverbund etablieren (5786). Neben den Befugnissen zur Erhebung und Auswertung von Daten soll auch die Vernetzung und der Datenaustausch unter den Sicherheitsbehörden (5789) sowie der Zugang zu relevanten privaten Datensammlungen wie z. B. von Bestandsdaten bei Providern verbessert werden (5873). Der Koalitionsvertrag enthält noch viele weitere Verbesserungen für die Arbeit der Sicherheitsbehörden.

Ausweitung der Videoüberwachung

Bezogen auf die Datenverarbeitung durch Behörden, um Straftaten zu verhüten, zu ermitteln, aufzudecken oder zu verfolgen oder um Strafen zu vollstrecken, muss der deutsche Gesetzgeber die JI-Richtlinie (EU) 2016/680, die die Europäische Union parallel zur Datenschutz-Grundverordnung erlassen hat, beachten. Dabei ist er jedoch an die Grundrechte der Grundrechtecharta und des Grundgesetzes gebunden. Er muss beachten, dass die geplanten Ausweitungen im Bereich der inneren Sicherheit Grundrechte einschränken. Die Ausweitung der Überwachungs- und Analysemöglichkeiten führt nicht nur dazu, dass Daten von Verdächtigen und Straftäterinnen und Straftätern verarbeitet werden, sondern auch die von vielen nicht verdächtigen und unschuldigen Bürgerinnen und Bürgern. Die geplanten Befugniserweiterungen müssen behutsam und grundrechtsschonend am Verhältnismäßigkeitsgrundsatz ausgerichtet werden. Nicht zu rechtfertigen sind Maßnahmen, die eine anlasslose, flächendeckende Überwachung der gesamten Bevölkerung ermöglichen. Die Weiterverarbeitung von erhobenen personenbezogenen Daten zu anderen Zwecken darf nur erlaubt sein, wenn die neue Nutzung der Daten spezifisch veranlasst ist und dem Schutz von Rechtsgütern oder der Aufdeckung von Straftaten mit besonderem Gewicht dient. Alle Befugnisse dürfen zusammengenommen nicht zu einer Totalüberwachung führen. Die Ausübung besonders eingriffsstarker Befugnisse sollten an einen Richtervorbehalt geknüpft werden.

Auswirkungen auf Grundrechte der Bürger beachten

Rechtsrahmen für autonomes Fahren

Zu begrüßen ist das Vorhaben der Koalition, einen Rechtsrahmen für autonomes Fahren zu schaffen, der Datenschutz und Datensicherheit ebenso gewährleistet wie ein Höchstmaß an Sicherheit (2143). Obwohl smarte Informationstechnologien, etwa Smart Cars, Smart Home oder Smart Health, mit enormen Risiken für das Grundrecht auf informationelle Selbstbestimmung verbunden sind, enthält die Datenschutz-Grundverordnung keine adäquaten risikospezifischen Regelungen, sondern stellt – wie auch für alle anderen Arten der Datenverarbeitungen – auf technikneutrale Regelungen ab. Gerade in komplexen und unübersichtlichen Datenverarbeitungssituationen, wie es bei Smart Cars der Fall ist, muss gewährleistet sein, dass die Betroffenen immer situationsadäquat darüber informiert sind, welche Daten überhaupt von wem verarbeitet werden. Ihnen sollen einfache Möglichkeiten zur Verfügung stehen, solchen Datenverarbeitungen zuzustimmen oder nicht. Dabei darf eine Nicht-Zustimmung nicht zu gravierenden Nachteilen führen.

Technik- und risikospezifische Regelung neuer Technologien

Rechtsrahmen für Smart Health

Die Koalition will das „bestehende E-Health-Gesetz im Zuge technologischer Innovationen im Dialog mit allen Akteuren" weiterentwickeln. Sie will als erste Schritte zur digitalen Patientenakte die Möglichkeit schaffen, den Impfpass, den Mutterpass und das Untersuchungsheft digital zu speichern und mit digitalen Rezepten arbeiten. Grundlagen für den sicheren Austausch dieser sensiblen Daten sollen „eine verlässliche und vertrauenswürdige Telematikinfrastruktur und höchste Datenschutz- und Datensicherheitsstandards" sein. Die Nutzung der digitalen Angebote soll „ausschließlich auf freiwilliger Basis (Opt-In)" erfolgen (2109ff., 4735ff.). Der Umgang mit Gesundheitsdaten erfordert höchste Datenschutz- und Datensicherheitsstandards. Diese müssen anwendungs- und risikospezifisch geregelt werden. Eine Bezugnahme auf die allgemeinen und abstrakten Regelungen der Datenschutz-Grundverordnung wäre unzureichend. Die Entscheidungsfreiheit der Betroffenen zu wahren ist der richtige Ansatz. Einer risikospezifischen Regelung, die vor Missbrauch schützt, bedürfen aber auch die vielen Gesundheitsdaten, die im Rahmen von freiwilligen Messverfahren für Körperfunktionen erhoben, (oft ins außereuropäische Ausland) übertragen und verarbeitet werden.

Technik- und risikospezifische Regelung neuer Technologien

Rechtsrahmen für Smart Cities

Die Koalition will „die Vorteile von Smart City und Smart Rural Area für die Menschen nutzbar machen". Sie will insbesondere mit Smart Grids und der Smart Meter-Technologie eine nachhaltige Energieerzeugung und -versorgung sicher und bedarfsgerecht gestalten und eine digitale Mobilitätsplattform errichten, die neue und existierende Mobilitätsangebote benutzerfreundlich miteinander vernetzt (2135). Diese Maßnahmen sind zur Verbesserung der Lebensqualität sowie des Umwelt- und Klimaschutzes zu begrüßen. Sie müssen aber auch sicherstellen, dass durch sie keine neuen und vertieften Risiken für die Privatheit und Selbstbestimmung der Betroffenen, insbesondere durch Verhaltens- und Bewegungsprofile, entstehen. Die Datenschutzregelungen im Messstellenbetriebsgesetz können hier als Vorbild dienen. Besondere Aufmerksamkeit sollte auf die datenschutzgerechte Systemgestaltung durch angemessene Datenverarbeitungsarchitekturen und durch Maßnahmen zur Datensparsamkeit[1] gelegt werden.

[1] S. hierzu das Forum Privatheit Policy Paper „Datensparsamkeit", 2017.

Digitalisierung und Selbstbestimmung

Neben den unmittelbar datenschutzbezogenen Vorhaben betreffen auch weitere im Koalitionsvertrag vorgesehene Maßnahmen indirekt die Rahmenbedingungen für Privatheit und Selbstbestimmung. Sie sind Gegenstand des folgenden Kapitels.

Eigentum an Daten

„Die Frage, ob und wie ein Eigentum an Daten ausgestaltet sein kann", will die Koalition „zügig angehen" (6107). Dieser Klärung greift der Koalitionsvertrag allerdings vor, indem er im Kapitel „Gesundheit und Pflege" feststellt, dass die Gesundheitsdaten Eigentum der Patientinnen und Patienten seien (4753).

Daten als Gegenstand einer gesellschaftlichen Kommunikationsordnung

Ob und wie ein Dateneigentum bestehen kann, ist in der Rechtswissenschaft noch umstritten. Einigkeit besteht, dass die Regelungen für Sacheigentum weder unmittelbar noch analog auf Daten übertragen werden können. Für personenbezogene Daten ist festzuhalten, dass sie Gegenstand der informationellen Selbstbestimmung und des Grundrechts auf Datenschutz sind und den Regelungen der Datenschutzgesetze unterliegen. An ihnen besteht kein Eigentum oder eigentumsgleiches Recht. Vielmehr sind sie Gegenstand einer gesellschaftlichen Kommunikationsordnung, die festlegt, wer in welchen Kontexten auf welche Weise mit diesen Daten umgehen darf. Hier stellt sich allenfalls die Frage, wie die betroffenen Personen an der Wertschöpfung im Umgang mit ihren Daten beteiligt werden können.

Soweit die Daten nicht personenbezogen sind, besteht ein gewisser Schutzbedarf, der seine Grundlagen z. B. in berechtigten Geheimhaltungsinteressen oder erbrachten Aufwänden, sie zu generieren, zu sammeln und zu ordnen, hat. Hierfür muss geprüft werden, ob und wie in der rechtlichen Kommunikationsordnung geeignete Ausschluss-, Verfügungs-, Schutz- und Entschädigungsrechte getroffen werden können.

Diskriminierungsverbote in der digitalen Welt

Zu begrüßen ist, dass der Koalitionsvertrag den Diskriminierungsverboten der „analogen Welt" auch in der digitalen Welt zu Gültigkeit verhelfen will (2097). Daher will die Koalition „zum Schutz der Verbraucherinnen und Verbraucher Algorithmen- und KI-basierte Entscheidungen, Dienstleistungen und Produkte überprüfbar machen, insbesondere im Hinblick auf mögliche unzulässige Diskriminierungen, Benachteiligungen und Betrügereien. ... Dynamische Preisbildung muss … nach klaren Regeln transparent dargestellt werden" (6373ff.).

Dieses wichtige Thema darf jedoch nicht allein auf den Verbraucherschutz reduziert werden. Die Verwendung von Algorithmen und Big Data etwa im Versicherungswesen oder in der Kreditvergabe ist zweifelsohne eine wichtige Frage. Auch ist mehr „Transparenz bei Online-Vergleichs- und Beratungsportalen" (2098) zu unterstützen. Nur wird die Beschränkung auf diese Anwendungsgebiete der Breite der Herausforderungen nicht gerecht. Die Verwendung von Algorithmen, KI und Big Data sowie die Vermessung und Katalogisierung des Menschen wird in allen Gesellschafts- und Wirtschaftsbereichen Einzug halten. Für jeden dieser Bereiche ist festzulegen, welche Bemessungskriterien und -verfahren zulässig und welche wegen der Gefahr von Diskriminierungen unzulässig sind.

Daten-Ethikkommission

Mögliche Abhilfe sieht der Koalitionsvertrag in einer Daten-Ethikkommission. Diese soll „Regierung und Parlament innerhalb eines Jahres einen Entwicklungsrahmen für Datenpolitik, den Umgang mit Algorithmen, künstlicher Intelligenz und digitalen Innovationen" vorschlagen. Dies ist mit der Hoffnung verbunden, dass die „Klärung datenethischer Fragen Geschwindigkeit in die digitale Entwicklung bringen und auch einen Weg definieren (kann), der gesellschaftliche Konflikte im Bereich der Datenpolitik auflöst" (2101ff.). Dass eine sachverständige und nicht nur Umsetzungsinteressen verhaftete Kommission sich mit diesen Fragen befasst, ist sehr zu begrüßen. Sie könnte Nutzen und Risiken dieser Technologien benennen und Regelungsoptionen darstellen. Dadurch könnte sie einen Anstoß bieten für eine breite gesellschaftliche Debatte zu allen Aspekten, die mit der Algorithmisierung von Individuum und Gesellschaft zusammenhängen. Ethische Fragen kommt aber nur dann eine breite praktische Wirkung zu, wenn sie mit interdisziplinären und anwendungsorientierten Untersuchung und Lösungsoptionen verbunden werden. Daher sollte die Kommission ausreichend interdisziplinär besetzt sein. Dabei darf es nicht um Konfliktbeschwichtigung im Interesse einer eindimensionalen Wirtschafts- und Technologieentwicklung gehen. Gesellschaftliche Konflikte im Bereich der Datenpolitik können in vielen Fällen nicht aufgelöst, aber in einem ersten Schritt bewusstgemacht und in weiteren Schritten bearbeitet werden. Dies erfordert eine breite gesellschaftliche Diskussion über eine verfassungs- und wertekonforme Gestaltung der Digitalisierung.

Daten als Gegenstand einer gesellschaftlichen Kommunikationsordnung

Die Frage nach der adäquaten Ausrichtung von Datenpolitik und dem richtigen Umgang mit Algorithmen und KI ist untrennbar auch mit Fragen nach der Konzentration technologischer, wirtschaftlicher und damit politischer und gesellschaftlicher Macht in den Händen einer kleinen Anzahl – gegenwärtig meist amerikanischer und chinesischer – Digitalkonzernen verbunden. Diese Problematik greift der Koalitionsvertrag an anderer Stelle durchaus auf, allerdings mit einem rein wettbewerbsrechtlichen Fokus. So wird die Einsetzung einer Kommission „Wettbewerbsrecht 4.0" versprochen, die Vorschläge zum Umgang der Marktmacht von Plattformunternehmen (vermutlich v. a. Facebook, Amazon und Google) unterbreiten soll (2776ff). Ebenso relevant wie ethische und wettbewerbsrechtliche Fragen ist daher, die Probleme der Konzentration gesellschaftlicher und politischer Macht bei den Digitalkonzernen ebenfalls in das Zentrum umfassender öffentlicher Debatten zu Fragen von Wertordnungen und legitimen Steuerungsverfahren einer digitalen Gesellschaft zu rücken.

Netzwerkdurchsetzungsgesetz

Die Koalition sieht im Netzwerkdurchsetzungsgesetz einen „richtigen und wichtigen Schritt zur Bekämpfung von Hasskriminalität und strafbaren Äußerungen in sozialen Netzwerken". Sie will auch weiterhin den „Schutz der Meinungsfreiheit sowie der Persönlichkeitsrechte der Opfer von Hasskriminalität und strafbaren Äußerungen sicherstellen. Die Berichte, zu denen die Plattformbetreiber verpflichtet sind, will die Koalition „sorgfältig auswerten und zum Anlass nehmen, um das Netzwerkdurchsetzungsgesetz insbesondere im Hinblick auf die freiwillige Selbstregulierung weiterzuentwickeln" (6196ff.) Außerdem will sie „die vertraglichen Rechte der Nutzer stärken, z. B. gegen unberechtigte Löschungen und Sperrungen" (6212).

Verbesserungen beim Schutz der Meinungsfreiheit

Das Netzwerkdurchsetzungsgesetz ist ein erster Schritt in die richtige Richtung. Die vorgesehenen Verbesserungen unterstützen die Entwicklung, die gesellschaftliche Verantwortung der Betreiber sozialer Netzwerke durchzusetzen.[1] Anerkannte Einrichtungen der regulierten Selbstregulierung können die Abwägung zwischen Meinungsfreiheit und Opferschutz neutral und professionell durchführen. Autorinnen und Autoren, die zu Unrecht blockiert wurden, müssen die Möglichkeit erhalten, ihre Rechte vor deutschen Gerichten einzuklagen, anstatt am Gerichtsstand (im der Regel in Kalifornien), den das soziale Netzwerk in seinen AGB vorgibt. Für einen effektiven Schutz der Betroffenen gegen Hass, Diskriminierung und Verleumdung im Netz müssen jedoch auch zusätzliche Kapazitäten geschaffen werden, um einerseits schnelle Rechtsschutzmöglichkeiten, insbesondere des einstweiligen Rechtsschutzes der Betroffenen zu ermöglichen und andererseits die bestehenden allgemeinen Vorschriften des Strafgesetzbuchs zu vollziehen und so eine effektive Strafverfolgung zu gewährleisten.

Digitale Bildungsoffensive

Die Koalition fordert eine „Digitale Bildungsoffensive", die sich auf die „gesamte Bildungskette" erstreckt. Sie soll „das gesunde Aufwachsen, die digitale Selbstbestimmung und individuelle aktive Teilhabe, den Umgang mit Daten sowie die hervorragende berufliche Bildung zum Ziel" haben (1716ff.). Zentral ist es hierbei, nicht lediglich Nutzungskompetenz, sondern ein umfassendes Verständnis der Digitalisierung zu vermitteln. Die Bildungsoffensive muss auch für die Wirkungen und Folgen der Digitalisierung sensibilisieren, die Tragweite der Nutzung bestimmter Dienste erkennen lassen und die Fähigkeit zu einem selbstbestimmten Handeln in der digitalen Welt vermitteln.

Forschung zur Digitalisierung

Zudem möchte die Koalition Forschungsförderung bezogen auf digitale Technologien verstärken. Hierzu will sie die Hightech-Strategie weiterentwickeln und „auf die großen gesellschaftlichen Herausforderungen" fokussieren. Dafür ist eine „Forschungsoffensive in allen Digitalisierungsfeldern" erforderlich. Als „besonders wichtig" erachtet der Koalitionsvertrag „Innovation, digitale Souveränität und Interdisziplinarität". Als Förderschwerpunkte werden jedoch nur technische Themen genannt (1767ff.). Wenn Lösungen für die großen gesellschaftlichen Herausforderungen gefunden und Schritte entwickelt werden sollen, die digitale Souveränität des Individuums und der Gesellschaft zu gewährleisten, müssen die interdisziplinären Forschungsanstrengungen auch auf die Gewährleistung von Privatheit und Selbstbestimmung, Demokratie und soziale Gerechtigkeit gerichtet werden.

[1] S. hierzu das Forum Privatheit Policy Paper „Das Netzwerkdurchsetzungsgesetz", 2018.

Ausblick

Der Koalitionsvertrag enthält viele gute Ansätze, um Innovation und Datenschutz zusammen zu fördern. Diese Ansätze sind nicht immer und überall im Vertrag auch ausreichend ausgeführt sowie mit geeigneten und effektiven Maßnahmen dargestellt. Das Policy Paper ergänzt die dargestellten Ansätze konstruktiv um konkretisierende und operative, bisweilen auch korrigierende Zielsetzungen und um geeignete Vorschläge für hilfreiche Umsetzungsmaßnahmen. Diese positiven Ergänzungen sind an dem übergeordneten Ziel ausgereichtet, durch Verbesserung der Verwirklichungsbedingungen von Privatheit und Selbstbestimmung sozialnützliche und wettbewerbstaugliche Innovationen hervorzubringen.

Die Erörterungen des Policy Papers orientieren sich an den Aussagen des Koalitionsvertrags. Dieser ist ein Dokument der politischen Machbarkeit innerhalb einer Legislaturperiode in der politischen Zusammenarbeit der beteiligten Parteien. Indem das Policy Paper die Ansätze des Koalitionsvertrags bewertet, präzisiert oder korrigiert, teilt es dessen Beschränktheit des Blicks auf die Probleme der Digitalisierung. Daher ist zum Abschluss darauf hinzuweisen, dass die Digitalisierung längerfristiger und in breiterer und tieferer Weise gesellschaftliche Infrastrukturen verändert und individuelle und kollektive Verhaltensweisen modifiziert, als es der Koalitionsvertrag thematisiert. Die wissenschaftliche Untersuchung der Auswirkungen der Digitalisierung auf die Verwirklichungsbedingungen von Privatheit und Selbstbestimmung muss sich also auch mit weitergehenden Analysen, Bewertungen, Lösungsvorschlägen und Gestaltungsempfehlungen beschäftigen.

forum <privatheit>
selbstbestimmtes_leben_in_der_digitalen_welt

GEFÖRDERT VOM

Bundesministerium für Bildung und Forschung

PROJEKTPARTNER

Fraunhofer

Natur Technik Kultur Gesellschaft UNIKASSEL VERSITÄT

provet
Projektgruppe verfassungsverträgliche Technikgestaltung

UNIVERSITÄT DUISBURG ESSEN
Offen im Denken

EBERHARD KARLS UNIVERSITÄT TÜBINGEN
INTERNATIONALES ZENTRUM FÜR ETHIK IN DEN WISSENSCHAFTEN

LMU LUDWIG-MAXIMILIANS-UNIVERSITÄT MÜNCHEN

ULD
Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein