Forum Privatheit und selbstbestimmtes Leben
in der digitalen Welt

MEHR FORTSCHRITT WAGEN – DURCH STÄRKUNG DES DATENSCHUTZES

Vorschläge zur Ausgestaltung des Koalitionsvertrags

Impressum

Mehr Fortschritt wagen – durch Stärkung des Datenschutzes: Vorschläge zur Ausgestaltung des Koalitionsvertrags

Autorinnen und Autoren

Alexander Roßnagel[1], Christian Geminn[1], Marit Hansen[2], Murat Karaboga[3], Michael Friedewald[3]

Institutionen

(1) Hessischer Beauftragter für Datenschutz und Informationsfreiheit, Projektgruppe verfassungsverträgliche Technikgestaltung im Wissenschaftlichen Zentrum für Informationstechnik-Gestaltung der Universität Kassel
(2) Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein, Kiel
(3) Fraunhofer-Institut für System- und Innovationsforschung ISI, Karlsruhe

Herausgeber

Michael Friedewald, Alexander Roßnagel, Christian Geminn, Murat Karaboga

Reihe

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

Veröffentlicht

Februar 2022, 1. Auflage
Fraunhofer-Institut für System- und Innovationsforschung ISI, Karlsruhe

Zitierempfehlung

Roßnagel u. a. (2022): Mehr Fortschritt wagen – durch Stärkung des Datenschutzes: Vorschläge zur Ausgestaltung des Koalitionsvertrags. Hrsg.: Michael Friedewald et al., Forum Privatheit und selbstbestimmtes Leben in der digitalen Welt, Karlsruhe: Fraunhofer ISI.

Hinweise

Dieses Werk ist lizenziert unter einer Creative Commons Namensnennung – Nicht kommerziell – Keine Bearbeitungen 4.0 International Lizenz. Die Autorinnen und Autoren gehen davon aus, dass die Angaben in diesem Bericht korrekt, vollständig und aktuell sind, übernehmen jedoch für etwaige Fehler, ausdrücklich oder implizit, keine Gewähr. Die Darstellungen in diesem Dokument spiegeln nicht notwendigerweise die Meinung des Auftraggebers wider.

Inhaltsverzeichnis

1 DIGITALE MODERNISIERUNG UND SELBSTBESTIMMUNG 7

2 SYSTEMWETTBEWERB UND DIGITALE SOUVERÄNITÄT 9
2.1 Werteorientierung in der digitalen Welt 9
2.2 Datentransfers in Drittstaaten 10

3 MODERNISIERUNG DES DATENSCHUTZES 12
3.1 Datennutzung und Datenschutz 12
3.2 Erleichterter Umgang mit Forschungsdaten 14
3.3 Weiterentwicklung des Datenschutzrechts 15
3.4 Regelungen zum Beschäftigtendatenschutz 15
3.5 Risikobasierte Überprüfung von KI-Anwendungen 16

4 STÄRKUNG DIGITALER BÜRGERRECHTE 18
4.1 Recht auf Verschlüsselung 18
4.2 Recht auf Anonymität 18
4.3 Schutz gegen IT-Schwachstellen 19

5 ÜBERWACHUNG UND FREIHEITSSCHUTZ 21
5.1 Überwachungsgesamtrechnung 21
5.2 Vorratsdatenspeicherung 22
5.3 Beschränkung von Überwachungssoftware 22
5.4 Biometrische Überwachung und Social Scoring 23

6 GESELLSCHAFTLICHER FORTSCHRITT DURCH DIGITALISIERUNG UND DATENSCHUTZ 25

1 DIGITALE MODERNISIERUNG UND SELBSTBESTIMMUNG

Der Koalitionsvertrag zwischen SPD, Bündnis 90/Die Grünen und FDP verspricht ein „Bündnis für Freiheit, Gerechtigkeit und Nachhaltigkeit". Die Koalition sieht sich „*am Beginn eines Jahrzehnts im Umbruch*".[1] Daher will sie „*nicht im Stillstand verharren*", sondern die „*notwendige Modernisierung*" von Staat und Gesellschaft „*vorantreiben*". Sie formuliert damit einen Gestaltungsanspruch, der sich vor allem auf die Digitalisierung von Wirtschaft und Gesellschaft bezieht. Digitalisierung verändert „*die Art und Weise, wie wir wirtschaften, arbeiten und miteinander kommunizieren*" (S. 3). 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 an vielen Stellen in Aussicht gestellt, erfordert für eine erfolgreiche Umsetzung jedoch konsequente Anstrengungen.

Jede Gestaltung der Digitalisierung muss zwei Ziele verfolgen: ihre Risiken mindern und ihre Chancen nutzen. Beides erfordert Innovationen. Politische Maßnahmen, die nur die Chancen im Blick haben, verfehlen die Aufgabe der umfassenden und verantwortlichen politischen Gestaltung. Diese Aufgabe formuliert auch der Koalitionsvertrag. Als politische Grundlage der Ampelkoalition aus drei Parteien, die von sich selbst sagen, dass sie „*unterschiedliche Traditionen und Perspektiven*" haben (S. 3), 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 Koalitionsvertrag nennt zahlreiche Vorhaben, die im weitesten Sinn Privatheit, Selbstbestimmung und Datenschutz betreffen oder Auswirkungen auf diese Werte haben. Mit ihrem Programm will die Koalition die Verwirklichungsbedingungen dieser Grundrechte nachhaltig verändern. Angesichts der Bedeutung dieses Programms hat der Expertenkreis „Forum Privatheit und selbstbestimmtes Leben in der digitalen Welt" den Koalitionsvertrag daraufhin analysiert, welche Aussagen er zur Gestaltung der Digitalisierung mit Blick auf die notwendige Modernisierung sowie Privatheit und Selbstbestimmung enthält. Für ausgewählte wichtige Aussagen des Koalitionsvertrags untersucht dieses 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 neuen Bundesregierung.

Sie stellt im Kapitel „Systemwettbewerb und digitale Souveränität" Maßnahmen vor, die Deutschland und Europa im globalen Wettbewerb um die Zukunft der Digitalisierung ergreifen müssen, um sich selbst behaupten und ihren eigenen Werten treu bleiben zu können.

Das Kapitel „Modernisierung des Datenschutzes" beschreibt Maßnahmen, die Deutschland umsetzen kann, um den Herausforderungen der Modernisierung durch Digitalisierung dadurch gerecht zu werden, dass es ihre Akzeptanz und Akzeptabilität durch den Schutz von Privatheit und Selbstbestimmung sicherstellt.

Das Kapitel „Stärkung digitaler Bürgerrechte" beschreibt Maßnahmen, die helfen, die Verwirklichungsbedingungen von Freiheit und Selbstbestimmung in einer digitalen Welt zu verbessern.

[1] Kursiv gesetzte Texte sind wörtliche Zitate aus dem Koalitionsvertrag, Zahlen in Klammern die Seitenzahlen, auf denen die Zitate zu finden sind.

Schließlich empfiehlt das Kapitel „Überwachung und Freiheitsschutz“ Maßnahmen, die Überwachungsinfrastrukturen so begrenzen, dass die notwendige Sicherheit von Einzelnen, Institutionen und Demokratie in einer Weise gewahrt werden kann, dass deren Freiheit keinen Schaden erleidet.

2 SYSTEMWETTBEWERB UND DIGITALE SOUVERÄNITÄT

„Im internationalen Systemwettstreit gilt es, unsere Werte entschlossen mit demokratischen Partnern zu verteidigen" (S. 3). Deutschland und die Europäische Union bauen ihre Demokratie auf den Grundrechten von Datenschutz und Selbstbestimmung auf. Diese sollen auch die freiheitliche Grundlage des Zusammenlebens in einer digitalen Welt sein.

2.1 Werteorientierung in der digitalen Welt

Der Koalitionsvertrag verfolgt bei der Digitalisierung auf allen Ebenen eine Orientierung an gesellschaftlichen Werten. „*Wir stärken die Digitalkompetenz, Grundrechte, Selbstbestimmung und den gesellschaftlichen Zusammenhalt. Wir sorgen für Sicherheit und Respekt auch in Zeiten des Wandels. Wir machen aus technologischem auch gesellschaftlichen Fortschritt. Dabei ist uns bewusst: Ein digitaler Aufbruch, der unsere Werte, die digitale Souveränität und einen starken Technologiestandort sichert, gelingt nur in einem fortschrittlichen europäischen Rahmen*" (S. 15). Im Einklang mit Digitalisierungsstrategien der Europäischen Union grenzt sich die Koalition mit dieser Zielsetzung von anderen globalen Entwicklungsmustern ab. Sie verfolgt zwischen dem von globalen US-amerikanischen Internetkonzernen praktizierten Digitalkapitalismus und dem von autoritären Staaten wie China betriebenen Entwicklungspfad eines digitalen Überwachungsstaats einen eigenen dritten Weg. Dieser zeichnet sich dadurch aus, dass er sich für die erforderliche digitale gesellschaftliche Transformation an der Stärkung der Grundrechte auf Datenschutz und Selbstbestimmung, der Verbesserung der Demokratie und der Verantwortung für die sozialen Folgen orientiert.

Angesichts der starken technologischen und wirtschaftlichen Abhängigkeit von Digitaltechnologie aus den USA können Europa und Deutschland diese angestrebte Werteorientierung aber nur verwirklichen, soweit sie für die Digitalisierung technologische Souveränität gewinnen, also tatsächlich frei sind, die digitale Transformation nach ihren Werten zu gestalten. Wie der EuGH in seinem Schrems II-Urteil vom 16. Juli 2020 für den Bereich des Grundrechtsschutzes festgestellt hat, ist dies mit Digitaltechnologie aus den USA bisher nicht möglich. Das Recht der USA ermöglicht den zuständigen Behörden, in einer unverhältnismäßigen Weise auf personenbezogene Daten aus Europa zuzugreifen, und schließt einen Rechtsschutz dagegen für US-Ausländer aus. Die Verwendung von US-Digitaltechnologie kann somit zu einem Grundrechtsverlust führen. Digitale Souveränität ist aber nicht nur eine Frage des Rechtsstaats und des Grundrechtsschutzes, sondern auch der Wettbewerbsfähigkeit, der politischen Selbstbestimmung und der Innovationskraft, der Entwicklung der Demokratie und der Verantwortung für die sozialen Folgen der Digitalisierung.

Um technologische Souveränität als Voraussetzung und Folge digitaler Selbstbehauptung zu erreichen, sind koordinierte Anstrengungen in vielen Politikbereichen wie der Wirtschafts- und Industrie-, Wettbewerbs-, Forschungs-, Bildungs-, Rechts- und Digitalpolitik in der Europäischen Union und in Deutschland erforderlich. Viele hilfreiche Maßnahmen werden vom Koalitionsvertrag angesprochen. Hierzu gehören technologische Souveränität als Forschungsziel (S. 20), die Förderung digitaler Schlüsseltechnologien (S. 18) wie Künstliche Intelligenz und Quantentechnologie, Cybersicherheit, Robotik, datenbasierte Lösungen quer durch alle Sektoren (S. 20) sowie die Unterstützung von IT-Sicherheit und DSGVO-konformer Datenverarbeitung (S. 19). „*Darüber hinaus sichern wir die digitale Souveränität, u. a. durch das Recht auf Interoperabilität und Portabilität sowie das Setzen auf offene Standards, Open Source und europäische Ökosysteme, etwa bei 5G oder KI*" (S. 16).

Zur digitalen Souveränität gehört auch die notwendige Abgrenzung: „*Nicht-vertrauenswürdige Unternehmen werden beim Ausbau kritischer Infrastrukturen nicht beteiligt*" (S. 17). Dabei ist zu berücksichtigen, dass Unternehmen, die ausländischer Gesetzgebung in der Weise unterliegen, dass sie verpflichtet sind, den Behörden ihres Heimatstaates auch gegen ihren Willen Daten zu übermitteln

und darüber Stillschwiegen zu wahren, wie „trojanische Pferde" wirken können, denen man die Funktion eines Datensammlers für ausländische Sicherheits- und Nachrichtendienste nicht ansieht. Dies ist u.a. bei US-amerikanischen und chinesischen Unternehmen und ihren Tochtergesellschaften in Europa der Fall.

Die konkreten Zielsetzungen digitaler Souveränität differieren nach Abhängigkeiten und nach Handlungsmöglichkeiten in den unterschiedlichen gesellschaftlichen Bereichen der Digitalisierung. Anzustreben sind z.B.

- Eigenentwicklungen von IT-Systemen und das Angebot von eigenen Plattformen und Diensten aus der Europäischen Union,
- der Eigenbetrieb ausländischer IT-Systeme durch europäische Verantwortliche (On-Premise-Lösungen),
- der Vertrieb, Support und Service ausländischer Informationstechnik durch Anbieter aus der Europäischen Union,
- die rechtskonforme Konfiguration ausländischer IT-Systeme unter Ausschluss von Datenübermittlungen in ein Drittland ohne ausreichendes Datenschutzniveau,
- der Einsatz von technisch-rechtlichen Treuhändern, die keinen ausländischen Stellen verpflichtet sind,
- ausreichende Transparenz über die Funktionen der IT-Systeme, insbesondere der erzwungenen Datenübermittlungen, und
- eine ausreichende eigene Bewertungssouveränität über Eigenschaften und Wirkungen von IT-Systemen und deren Risiken.

Welche Zielsetzung als passend und ausreichend angesehen werden kann, ist für das jeweilige politische, wirtschaftliche und technische Handlungsfeld festzulegen.

Inwieweit digitale Souveränität erreicht wird, hängt stark vom Investitions- und Konsumverhalten ab. Entscheidend dafür ist, ob es äquivalente Angebote aus Europa oder Deutschland auf dem Markt gibt und wie diese nachgefragt werden. Der Bund sollte in seiner Rechtspolitik geeignete Rahmenregelungen für die Entwicklung und Unterstützung von alternativen Technikanwendungen festlegen und für seinen eigenen Bereich das Angebot alternativer Produkte und Dienstleistungen koordinieren. So sollte z.B. Rechtskonformität mit den Schrems II-Vorgaben Voraussetzung in jedem Vergabeverfahren sein. Hier können öffentliche Stellen des Bundes als Vorbild mit guten Beispielen auch für Techniknutzungen in der Wirtschaft und im Konsumbereich vorangehen. Ein solches Beispiel spricht der Koalitionsvertrag auf S. 15 an: *„Auf Basis einer Multi-Cloud Strategie und offener Schnittstellen sowie strenger Sicherheits- und Transparenzvorgaben bauen wir eine Cloud der öffentlichen Verwaltung auf."* Schließlich kann der Bund mit Aufklärung, Beratung und Unterstützung dafür sorgen, dass auch andere Verantwortliche alternative IT-Systeme einsetzen können.

2.2 Datentransfers in Drittstaaten

Der Koalitionsvertrag greift den Transfer personenbezogener Daten in Drittstaaten jenseits des Europäischen Wirtschaftsraums auf. Die Koalitionäre wollen sich für *„ein ambitioniertes Abkommen mit den USA*" einsetzen, *„das einen rechtssicheren und datenschutzkonformen Datentransfer auf europäischem Schutzniveau ermöglicht*" (S. 35). Gleichzeitig soll die grenzüberschreitende polizeiliche und justizielle Zusammenarbeit intensiviert werden. Hohe Datenschutzstandards und grenzüberschreitender Rechtsschutz sollen dabei jedoch gewährleistet werden (S. 105). Diese Bemühungen hin zu einer Ausweitung von Datentransfers dürfen indes nicht dazu führen, dass das Ziel des Koalitionsvertrags, digitale Souveränität zu sichern, untergraben wird.

Konkret bedeutet dies, dass ein dritter Anlauf eines rechtmäßigen Angemessenheitsbeschlusses bezogen auf die USA nach den vom EuGH als unionsrechtswidrig aufgehobenen Abkommen „Safe Harbor" und „Privacy Shield" eine echte Weiterentwicklung des Grundrechtsschutzes darstellen und

eng an den Vorgaben des EuGHs in seinem Schrems II-Urteil ausgerichtet sein muss. Diese Vorgaben können nur erfüllt werden, wenn es in den USA zu substanziellen Änderungen insbesondere des Rechtsrahmens der Datenverarbeitung durch Behörden für öffentliche Sicherheit und Ordnung und der Nachrichtendienste kommt. Außerdem darf es keine Zugriffs- oder Herausgaberechte der US-Behörden auf Daten geben, die in Europa verarbeitet werden, auch wenn dies durch US-amerikanische Unternehmen und deren Tochtergesellschaften erfolgt. Schließlich muss betroffenen Personen auch dann Rechtsschutz gegen eine unzulässige Datenverarbeitung gewährt wird, wenn sie keine US-Bürger sind.

3 MODERNISIERUNG DES DATENSCHUTZES

Die Chancen der Digitalisierung zu nutzen, setzt die zunehmende Verarbeitung von personenbezogenen und nicht personenbezogenen Daten voraus. Dies wird zu einem veränderten gesellschaftlichen und individuellen Umgang mit Daten führen. Digitalisierung soll aber die Grundlagen für ein selbstbestimmtes Leben nicht gefährden. Um beide Ziele – Digitalisierung und Selbstbestimmung – zu erreichen, sind Gestaltungen der Datenverarbeitungen und Modernisierungen im Datenschutz erforderlich, die aufeinander bezogen sind.

3.1 Datennutzung und Datenschutz

Eine Frage der digitalen Souveränität ist auch die Verfügung über Daten, um Auswertungen durch Künstliche Intelligenz und Big Data-Anwendungen zu ermöglichen. Um ihre selbstlernenden Systeme zu trainieren und zu evaluieren, sind Anwender von Künstlicher Intelligenz und Big Data auf sehr viele Daten angewiesen, die sie normalerweise nicht alle selbst erheben können. Solche Daten müssen in allgemeinen, für jeden Interessierten zugänglichen „Datenräumen" gesammelt werden, damit für Technikentwicklungen für Gemeinwohlinteressen – wie Forschung, Gesundheitsversorgung oder Infrastrukturplanungen – genügend Daten zur Verfügung stehen. Hierfür will der Koalitionsvertrag vorsorgen: „*Die Potenziale von Daten für alle heben wir, indem wir den Aufbau von Dateninfrastrukturen unterstützen und Instrumente wie Datentreuhänder, Datendrehscheiben und Datenspenden gemeinsam mit Wirtschaft, Wissenschaft und Zivilgesellschaft auf den Weg bringen. Wir streben einen besseren Zugang zu Daten an, insbesondere um Start-ups sowie KMU neue innovative Geschäftsmodelle und soziale Innovationen in der Digitalisierung zu ermöglichen. Ein Dateninstitut soll Datenverfügbarkeit und -standardisierung vorantreiben, Datentreuhändermodelle und Lizenzen etablieren. Für Gebietskörperschaften schaffen wir zu fairen und wettbewerbskonformen Bedingungen Zugang zu Daten von Unternehmen, insofern dies zur Erbringung ihrer Aufgaben der Daseinsvorsorge erforderlich ist. Für alle, die an der Entstehung von Daten mitgewirkt haben, stärken wir den standardisierten und maschinenlesbaren Zugang zu selbsterzeugten Daten. Mit einem Datengesetz schaffen wir für diese Maßnahmen die notwendigen rechtlichen Grundlagen*." (S. 17)

In diesem künftigen Datengesetz – das mit dem künftigen Data Governance Act (DGA) der Europäischen Union abgestimmt sein muss – sollte die Koalition berücksichtigen, dass solche Datenräume bereits existieren – allerdings in privater Hand. Globale Plattformen wie Google, Amazon, Facebook, Microsoft, Apple, Alibaba und Tencent speichern extrem große Sammlungen personenbezogener Daten von Kunden – und auch Nichtkunden. Die Plattformen nutzen diese Daten nicht nur, um Persönlichkeitsprofile zu erstellen und diese für individualisierte Werbung zu nutzen, sondern auch, um mit den Datenpools innovative Techniken und Geschäftsmodelle zu entwickeln. Ausreichende Schutzvorkehrungen für betroffene Personen fehlen. Ihren Datenschatz stellen diese Plattformen nicht der Allgemeinheit zur Verfügung, sondern nutzen ihn ausschließlich für ihre eigenen Zwecke. Diese Datenmacht gibt ihnen Wettbewerbsvorteile, die sich negativ auf die Innovations- und die Wettbewerbsfähigkeit ihrer Konkurrenten auswirken. Die Koalition sollte daher prüfen, inwieweit sie – wenn möglich im europäischen Rahmen – diese Plattformen verpflichten kann, ihre Datenpools anonymisiert gemeinnützigen Zwecken zur Verfügung zu stellen. Die Datensammlungen könnten dann genutzt werden, um z.B. Gesundheits-, Gesellschafts-, Verkehrs-, Ressourcen-, Energie- und Umweltforschung zu ermöglichen oder zu verbessern.

Unabhängig von diesen privatisierten Datenräumen will der DGA allgemeine öffentliche Datenräume fördern. Für den notwendigen Grundrechtsschutz der betroffenen Personen, deren Daten – personenbezogen oder anonymisiert – in die Datenräume eingestellt werden, ist zu beachten, dass weder der DGA noch die DSGVO, auf die der DGA verweist, den Grundrechtsschutz in diesen „Da-

tenräumen" ausreichend gewährleisten. Soweit der deutsche Gesetzgeber sich auf Öffnungsklauseln berufen kann (z.B. Art. 6 Abs. 2 und 3 in Verbindung mit Abs. 1 UAbs. 1 Buchst. e oder Art. 9 Abs. 2 Buchst. j DSGVO), sollte er sektorspezifische Regelungen treffen, die den besonderen Zwecken (z.B. Gesundheitsforschung, Energieeinsparung oder Mobilität) und den spezifischen Risiken gerecht werden. Um die notwendigen Ergänzungen zu bestimmen, ist es sinnvoll, zwischen personenbezogenen und nicht-personenbezogenen Daten zu unterscheiden.

Personenbezogene Daten können die Akteure in den Datenräumen (Datentreuhänder, Datendrehscheiben, Datengenossenschaften und Datenspender) auf der Grundlage einer Einwilligung oder eines (Verwertungs-)Vertrags sammeln und weitergeben. Als ausreichende Vorgaben zum Schutz der Grundrechte der betroffenen Personen gegenüber den spezifischen Risiken der Verwendung von Daten für KI-Systeme wären z.B. Bestimmungen notwendig, welche Verarbeitungszwecke im Allgemeininteresse liegen, welche Vertragsbedingungen zulässig oder zwingend sind, welche Technikgestaltungen angeboten werden müssen (z.B. On-Premise-Auswertungen) und welche technischen Schutzvorkehrungen erforderlich sind. Um die Datennutzung sinnvoll auf eine Einwilligung stützen zu können, ist unter anderem festzulegen, wie die betroffenen Personen regelmäßig über die Verwendung der von ihnen bereitgestellten Daten zu informieren sind, wie sie eine ursprünglich breite Einwilligung später präzisieren können (dynamische Einwilligung), wie lange eine Einwilligung gültig ist und wie Zweckbindungen (z.B. „nur für Corona-Forschung", „nur für Straßenplanung", „nur für meine Gemeinde") gesichert werden. Schließlich ist festzulegen, für welche Akteure Zeugnisverweigerungsrechte und Beschlagnahmeverbote vorzusehen sind.

Mit den europäischen Gesetzesinitiativen zu einer verstärkten Nutzung und Teilung von Daten ist darauf zu achten, inwieweit Datenbestände eine Personenbeziehbarkeit ermöglichen und damit das Datenschutzrecht zu beachten ist. Auch für vermeintlich anonymisierte Datensammlungen war es in der Vergangenheit schon oft möglich, einen Personenbezug herzustellen. Dieses Risiko verstärkt sich noch, wenn weitere Informationen verfügbar sind, die durch eine Verknüpfung oder Inferenzen zu einer Identifizierung einzelner oder vieler Personen beitragen. Aus diesem Grund kommt der Förderung von effektiven Anonymisierungstechniken eine hohe Bedeutung zu, wie auch der Koalitionsvertrag betont: „*Wir fördern Anonymisierungstechniken (und) schaffen Rechtssicherheit durch Standards*." (S. 17)

Der Aspekt der Rechtssicherheit für die Anwender, die nicht-personenbezogene Daten bereitstellen oder nutzen wollen, spielt eine große Rolle, denn es ist nicht trivial, einen Datenbestand auf etwaigen Personenbezug zu prüfen oder einen solchen durch Anonymisierung zuverlässig zu entfernen. Für die Anwender ist es wichtig zu wissen, ob sie dem Regime des Datenschutzrechts unterliegen und die damit verbundenen Anforderungen erfüllen müssen. Es ist zu begrüßen, wenn Standards erarbeitet werden, die das Risiko für die Anwender vermeiden, fälschlich davon auszugehen, dass sie nicht-personenbezogene Daten verarbeiten, und wegen Datenschutzverstößen belangt zu werden.

Daten, die zuvor anonymisiert worden sind, können gesammelt und geteilt werden. Hierfür sind höchste Standards der Anonymisierung zu wählen. Der Einsatz von Anonymisierungstechniken alleinreicht jedoch nicht aus, um dauerhaft vertrauenswürdige und rechtssichere Lösungen zu garantieren. Denn die weitere Entwicklung der Informationstechnik führt immer wieder zu neuen Risiken für die Wahrung der Anonymität. Daher muss auch mit von heute aus nicht vorhersehbaren Re-Identifizierungen gerechnet werden – insbesondere dann, wenn die Daten vielen Verantwortlichen mit unterschiedlichem Zusatzwissen zur Verfügung stehen und langfristig aufbewahrt und damit dem künftigen technischen Fortschritt der Re-Identifizierung ausgesetzt sein werden. Wenn ausreichendes Vertrauen in die Anonymisierung erreicht werden soll, müssen die Anonymisierungsverfahren um – insbesondere rechtliche – Vorsorgemaßnahmen ergänzt werden. Zu diesen Maßnahmen könnte beispielsweise gehören, eine De-Anonymisierung – etwa nach japanischem Vorbild – zu verbieten. Dieser Punkt ist im Koalitionsvertrag aufgenommen worden, indem er die Einführung

einer „*Strafbarkeit rechtswidriger De-anonymisierung*" ankündigt (S. 17). Weitere Vorsorgemaßnehmen können etwa umfassen, die Weitergabe und Weiterverarbeitung anonymisierter Daten zu beschränken, eine Zweckbindung für anonymisierte Daten (sofern die Einwilligung oder der Verwertungsvertrag eine solche enthalten) vorzusehen oder die anonymisierten Daten zu löschen, sobald sie nicht mehr benötigt werden.

Bei Einführung einer Strafbarkeit einer rechtswidrigen De-Anonymisierung sind vorab etwaige unerwünschte Nebeneffekte zu prüfen. Ausnahmen sollte es im Bereich der Forschung zu Informationssicherheit und Datenschutz geben, bei der es gerade darum geht, die vorhandenen Risiken zu verstehen und Abhilfemaßnahmen zu entwickeln. So darf eine solche Regelung auch nicht dazu führen, dass man mögliche technisch-organisatorische Verbesserungen bei einer Anonymisierung oder beim Schutz personenbezogener Daten unterlässt.

3.2 Erleichterter Umgang mit Forschungsdaten

„*Wissenschaft- und Forschungsfreiheit sind der Schlüssel für kreative Ideen, die dazu beitragen, die großen Herausforderungen unserer Zeit zu bewältigen*" (S. 8). Von besonderer Bedeutung ist daher der Zugang und der Umgang mit Forschungsdaten. Hierzu sieht der Koalitionsvertrag (S. 21) vor: „*Das ungenutzte Potential, das in zahlreichen Forschungsdaten liegt, wollen wir effektiver für innovative Ideen nutzen. Den Zugang zu Forschungsdaten für öffentliche und private Forschung wollen wir mit einem Forschungsdatengesetz umfassend verbessern sowie vereinfachen und führen Forschungsklauseln ein. Open Access wollen wir als gemeinsamen Standard etablieren. … Die Nationale Forschungsdateninfrastruktur wollen wir weiterentwickeln und einen Europäischen Forschungsdatenraum vorantreiben. Datenteilung von vollständig anonymisierten und nicht personenbezogenen Daten für Forschung im öffentlichen Interesse wollen wir ermöglichen*."

Für diese Forschungsdaten gelten die Ausführungen zu allgemeinen Datenräumen (s. vorstehend) gleichermaßen. Forschungsdaten sind für Fortschritte der Gesellschaft von besonderer Bedeutung. Daher wird der Umgang mit ihnen in der DSGVO bereits erheblich erleichtert. Wenn der Zugang zu ihnen weiter verbessert und vereinfacht werden soll, ist zu berücksichtigen, dass dadurch besondere Risiken entstehen, gegen die Vorkehrungen zu treffen sind. Denn zu Forschungsdaten können alle Daten werden, wenn Forschende sie dazu machen. Für Forschung interessant sind vor allem besondere Kategorien von personenbezogenen Daten, die besonderen Schutz benötigen, wie Gesundheitsdaten, biometrische oder genetische Daten oder Daten zum sexuellen Verhalten, zu politischen Meinungen sowie zu religiösen oder weltanschaulichen Überzeugungen (Art. 9 Abs. 1 DSGVO). Schließlich müssen Forschungsdaten unter Forschenden geteilt werden können, für weitere Forschungen nachnutzbar sein, für Längsschnittstudien zum Teil sehr lange aufbewahrt werden und gegebenenfalls in der Kommunikation mit den betroffenen Personen zur Verfügung stehen. Dieser notwendige Umgang mit Forschungsdaten ist mit besonderen Risiken für die informationelle Selbstbestimmung der betroffenen Personen verbunden.

Aufgrund dieser besonderen Risiken ist bei der Erleichterung der Forschung in besonderer Weise darauf zu achten, dass der Grundrechtsschutz der betroffenen Personen ausreichend gewahrt wird. Dafür kann erforderlich sein, dass Forschende einem Berufsgeheimnis unterliegen wie etwa Ärzte, Rechtsanwälte oder Steuerberater. Dies hätte zum einen zur Folge, dass die Forschenden zu geeigneten Maßnahmen zum Schutz der Forschungsdaten verpflichtet sind. Zum anderen wären sie dann gegen Herausgabeansprüche von Arbeitgebern oder staatlichen Stellen geschützt.

Auch der Umgang mit Forschungsdaten sollte den spezifischen Risiken entsprechend geregelt werden. Die sehr abstrakten, allgemeinen Regelungen der DSGVO sind dafür unzureichend. Die Öffnungsklauseln der Art. 6 Abs. 2 bis 4, 9 Abs. 2 Buchst. j sowie 89 DSGVO geben hierfür einen gewissen Spielraum. Wenn die Zweckbindung personenbezogener Daten gelockert oder aufgehoben ist, wenn die Daten zu Forschungszwecken benötigt werden, müsste im Gegenzug eine strikte

Zweckbegrenzung der Forschungsdaten nur für Forschungszwecke bestehen. Um Missbrauch zu verhindern, sollte auch festgelegt werden, was als Forschung gilt und wer als forschende Person erleichterten Zugang zu Forschungsdaten haben soll. Auch ist zu regeln, welche wissenschaftlichen Ethikstandards eingehalten werden müssen und wie diese überprüft werden. Um Missbrauch zu vermeiden, ist festzulegen, inwieweit Unternehmen, Journalisten und zivilgesellschaftliche Organisationen als Forschende anzusehen sind. Die Anforderungen an den Schutz der Daten durch Sicherheitsvorkehrungen und Pflichten der Forschenden muss ebenfalls geregelt werden. Für Datenmittler und Treuhänder von Forschungsdaten ist eine strikte Verpflichtung der auf Neutralität und Einhaltung der Betroffenenrechte erforderlich.

3.3 Weiterentwicklung des Datenschutzrechts

Auch jenseits der Erleichterung der Datennutzung und des Umgangs mit Forschungsdaten sind Weiterentwicklungen des Datenschutzrechts angezeigt. Zutreffend heißt es im Koalitionsvertrag, die DSGVO sei „*eine gute internationale Standardsetzung*". Es stecken große Potenziale zur Stärkung von europäischen wie auch deutschen Grundrechten und -werten in der Verordnung selbst und in damit verbunden Bereichen wie etwa der Überführung der ePrivacy-Richtlinie in eine Verordnung (S. 17). Insgesamt wären weitere Konkretisierungen wünschenswert. Ein Beispiel ist die Stärkung des datenschutzrechtlichen Schutzes von Kindern. So könnte betont werden, dass die Interessen eines Kindes bei der Prüfung der Vereinbarkeit eines neuen Verarbeitungszwecks nach Art. 6 Abs. 4 DSGVO, beim Recht auf Widerspruch nach Art. 21 Abs. 1 und 6 DSGVO, in der Datenschutz-Folgenabschätzung nach Art. 35 DSGVO und bei einer notwendigen Neufassung der Altersregelung in Art. 8 Abs. 1 DSGVO besondere Berücksichtigung erfahren sollten. Bestimmte Verarbeitungen von Kinderdaten wie für Werbezwecke und Profiling, die Einwilligung eines Kindes in automatisierte Entscheidungen nach Art. 22 Abs. 2 Buchst. c DSGVO und in die Verarbeitung besonderer Kategorien personenbezogener Daten nach Art. 9 Abs. 2 Buchst. a DSGVO könnten ausdrücklich ausgeschlossen werden.

Auch zu anderen Datenschutzthemen wären Weiterentwicklungen des Datenschutzrechts sinnvoll, beispielsweise bezüglich des Rechts auf Datenübertragbarkeit (Art. 20 DSGVO) oder der Verpflichtung zu Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen (Art. 25 DSGVO), um die Ziele, die in diesen Regelungen zum Ausdruck kommen, besser verwirklichen zu können und Rechtssicherheit für alle Beteiligten zu erreichen (s. Roßnagel/Geminn, Datenschutz-Grundverordnung verbessern, 2020).

Zur Gewährleistung von Rechtssicherheit trüge auch die Verpflichtung des Herstellers zu einer datenschutzgerechten Systemgestaltung bei (s. DSK, Erfahrungsbericht zur Anwendung der DSGVO, 2019, S. 16f.). In all diesen Bereichen könnten Impulse von den Mitgliedstaaten ausgehen.

3.4 Regelungen zum Beschäftigtendatenschutz

Eine konkrete Weiterentwicklung des Datenschutzrechts sieht der Koalitionsvertrag allerdings nur im Bereich des Beschäftigtendatenschutzes vor, wo (nicht zum ersten Mal) dedizierte Regelungen angekündigt werden, „*um Rechtsklarheit für Arbeitgeber sowie Beschäftigte zu erreichen und die Persönlichkeitsrechte effektiv zu schützen*" (S. 17). So hatte auch der Koalitionsvertrag von CDU/CSU und SPD aus dem Jahr 2018 angekündigt, die damalige Koalition wolle „die Schaffung eines eigenständigen Gesetzes zum Beschäftigtendatenschutz" prüfen, „das die Persönlichkeitsrechte der Beschäftigten am Arbeitsplatz schützt und Rechtssicherheit für den Arbeitgeber schafft" (Koalitionsvertrag 2018, S. 129). Mit Art. 88 Abs. 1 DSGVO ermöglicht die Verordnung den Mitgliedstaaten explizit den Erlass spezifischerer Vorschriften hinsichtlich der Verarbeitung personenbezogener Beschäftigtendaten im Beschäftigungskontext. Im Zentrum müssen dabei die Rechte und Freiheiten der Beschäftigten stehen.

Wie in unserem Policy Paper zum Koalitionsvertrag von 2018[2] empfohlen, sollte die neue Bundesregierung risikoadäquate Datenschutzregelungen treffen, die heimliche Kontrollen von Beschäftigten ebenso explizit ausschließen wie eine Dauerüberwachung und die Erstellung umfassender Bewegungsprofile. Ebenso sollte ihre Lokalisierung 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.

Ein schlichtes Anknüpfen an die Diskussion des Beschäftigtendatenschutzes vor zehn Jahren kann deshalb nicht zum Erfolg führen. Es muss vielmehr – auf der Basis der Arbeiten des Beirats für Beschäftigtendatenschutz beim BMAS – eine umfassende Evaluation aktueller und auch zukünftiger Herausforderungen erfolgen. Diesen Herausforderungen wird die rudimentäre Regelung in § 26 BDSG nicht gerecht. Die DSK nennt als kritische Bereiche etwa das Fragerecht im Kontext von Bewerbungen, das sog. „Pre-Employment-Screening", die biometrische Authentifizierung und Autorisierung sowie die Geolokalisation von Beschäftigten (s. Kurzpapier Nr. 14, S. 4). Die Regulierung digitaler Plattformen hinsichtlich guter und fairer Arbeitsbedingungen und die Gestaltung des Einsatzes von KI in der Arbeitswelt auf der Grundlage eines menschenzentrierten Ansatzes mit dem Ziel sozialer und wirtschaftlicher Innovation und Gemeinwohlorientierung (S. 85) sind zwei Vorhaben der Koalition, die zu unterstützen sind.

Damit ist klar, dass technologieneutrale, aber dennoch risikospezifische Regelungen für zahlreiche Verarbeitungskonstellationen im Beschäftigungskontext geschaffen werden müssen, bei denen der Gesetzgeber auch bereits Risikoeinschätzungen vorwegnimmt. Ein Vorbild für solche Regelungen könnte § 4 BDSG sein, der eine bereichsspezifische Regelung für die Videoüberwachung öffentlich zugänglicher Räume enthält.

3.5 Risikobasierte Überprüfung von KI-Anwendungen

„*Wir unterstützen den europäischen AI Act. Wir setzen auf einen mehrstufigen risikobasierten Ansatz, wahren digitale Bürgerrechte, insbesondere die Diskriminierungsfreiheit, definieren Haftungsregeln und vermeiden innovationshemmende ex-ante-Regulierung*" (S. 18, 72).

Die Orientierung an dem risikobasierten Ansatz des EU AI Acts ist unterstützenswert. Bedeutung erlangt der vorgesehene risikobasierte Ansatz allerdings erst durch die unterschiedliche regulatorische Behandlung verschiedener KI-Verarbeitungen in Abhängigkeit von ihrer jeweiligen Risiko-Klassifizierung. Insofern muss ex-ante-Regulierung Teil eines solchen KI-Gesetzes sein – nichts Anderes stellen schließlich der AI Act selbst und auch das im Koalitionsvertrag vorgesehene Verbot biometrischer Erkennung im öffentlichen Raum und automatisierter staatlicher Scoring-Systeme dar. Insofern darf die Förderung der Überprüfbarkeit algorithmischer Systeme nicht allein auf den Bereich des Digital Services Acts (S. 17) begrenzt werden, sondern sollte auch im Bereich der Eindämmung der durch KI-Einsatz generierten Risiken Anwendung finden.

Im Rahmen des KI-Gesetzgebungsprozesses ist zunächst entscheidend, wie die Risikodifferenzierung erfolgt und an welchem Punkt die Grenze zwischen extrem riskanten verbotenen und sehr riskanten, aber nicht verbotenen KI-Anwendungen gezogen wird. Sobald diese Grenze unionsrechtlich bestimmt wurde, gilt es, die Bewertung des spezifischen Risikos der erlaubten sehr riskanten

[2] Roßnagel, A.; Bile, T.; Geminn, C.; Johannes, P. C.; Karaboga, M.; Krämer, N.; Maier, N.; Martin, N.; Müller, J.; Nebel, M.; Friedewald, M.; Bremert, B. (2018). Datenschutz stärken, Innovationen ermöglichen: Wie man den Koalitionsvertrag ausgestalten sollte. Policy Paper. Karlsruhe: Forum Privatheit und selbstbestimmtes Leben in der digitalen Welt

Verarbeitungen vorzunehmen, sodass auf Verarbeitungen, die ein besonderes Risiko für Gesellschaft und Individuum mit sich bringen, reagiert werden kann. Weil es sich bei KI-Anwendungen und ihren Risiken um ein typisches moving target-Problem handelt, werden staatliche Stellen und der Gesetzgeber nicht in der Lage sein, die Vielzahl der in den kommenden Jahren zu erwartenden KI-Anwendungen im Hinblick auf ihre Kritikalität zu evaluieren, sodass eine fehlende oder zu späte Reaktion auf neue Risiken zu erwarten ist. Hierbei kommt der Forschung und unabhängigen Institutionen aus unterschiedlichen gesellschaftlichen Bereichen wie Datenschutzbehörden eine zentrale Rolle zu.

4 STÄRKUNG DIGITALER BÜRGERRECHTE

„Wir stärken digitale Bürgerrechte und IT-Sicherheit. Sie zu gewährleisten ist staatliche Pflicht. Wir führen ein Recht auf Verschlüsselung, ein wirksames Schwachstellenmanagement, mit dem Ziel Sicherheitslücken zu schließen, und die Vorgaben „security-by-design/default" ein. Auch der Staat muss verpflichtend die Möglichkeit echter verschlüsselter Kommunikation anbieten. Hersteller haften für Schäden, die fahrlässig durch IT-Sicherheitslücken in ihren Produkten verursacht werden." (S. 16)

Diese Festlegungen entsprechen der Werteorientierung der digitalen Transformation, wie sie im gesamten Koalitionsvertrag zum Ausdruck kommt. Der Schutz der Bürgergrundrechte bleibt auch bei der Gewährleistung innerer Sicherheit als Sicherheitsziel an erster Stelle und wird nicht instrumentellen Zwängen und Nöten untergeordnet. Dies ist aus dem Blickwinkel des Grundrechtsschutzes sehr zu begrüßen. Die Stärkung digitaler Bürgerrechte ist ein wichtiger Vertrauensbaustein für das Gelingen der digitalen Transformation als gesellschaftlicher Fortschritt.

4.1 Recht auf Verschlüsselung

Die Einführung eines Rechts auf Verschlüsselung knüpft an die Entscheidung der Bundesregierung zur Krypto-Debatte um die Jahrtausendwende an, auf Verschlüsselung als Grundlage sicherer Kommunikation im digitalen Raum zu setzen. Dieser lag die Erkenntnis zugrunde, dass eine Schwächung von Verschlüsselungsverfahren auch von böswilligen Dritten genutzt werden könnte und die gesamte Sicherheit der Kommunikation und Datenverarbeitung in Wirtschaft und Verwaltung gefährden würde. Gerade die digitale Transformation ist darauf angewiesen, dass alle Beteiligten auf eine sichere Kommunikation und Datenspeicherung vertrauen können.

Das Recht auf Verschlüsselung soll zum einem als Abwehrrecht ausgestaltet werden. Das heißt dass der Staat weder geheime Schlüssel herausfordern noch verlangen darf, dass Verschlüsselungsverfahren verwendet werden müssen, die für Behörden ausnutzbare Schutzlücken aufweisen. Dieses Recht hat zum anderen eine Freiheitsdimension, als frei gewählt werden darf, welche Verschlüsselungsverfahren zum Einsatz kommen. Schließlich hat dieses Recht auch eine Leistungsdimension, als der Staat für die Kommunikation mit ihm die Möglichkeit echter verschlüsselter Kommunikation anbieten muss. „Echte Verschlüsselung" sollte dabei so gemeint sein, dass sie nicht über bekannte Schwachstellen verfügt, die staatliche Behörden ausnutzen können. Schließlich ist mit diesem Recht eine Schutzpflicht des Staates verbunden, durch Ge- und Verbote, Standardisierung und Aufklärung eine ungehinderte und nichtkompromittierte Verschlüsslung zu gewährleisten. Dem widerspricht es nicht, wenn die Koalition den Betreibern und Anbietern von IT-Diensten und Verantwortlichen von Datenverarbeitungen Verschlüsselungspflichten auferlegt, um „security-by-design-and-by-default" durchzusetzen.

Hervorzuheben ist, dass der Koalitionsvertrag auf S. 108 den Kampf gegen Kinderpornografie und Kindesmissbrauch thematisiert, ohne die Entschlüsselung von Internet-Diensten vorzusehen. Dies erfolgt im Gegensatz zu Forderungen der Europäischen Kommission, die entsprechende Pflichten für die Betreiber von Messenger-Diensten einführen will.

4.2 Recht auf Anonymität

Zur freien Entfaltung der Persönlichkeit ist es wichtig, dass nicht jede Bewegung und jede Handlung mit einer Identifizierung der Person verbunden ist. Anonymität in der digitalen Welt, z.B. beim Surfen im Internet, ist aufgrund der technischen Datenspuren, die zur Diensteerbringung erforderlich sind, und der darüber hinaus gesammelten Daten in der heutigen Praxis keine Selbstverständlichkeit mehr. Auch nimmt auch die Identifizierbarkeit und Nachverfolgbarkeit von Menschen beim

Bewegen im öffentlichen Raum durch den Einsatz von Überwachungstechnik und durch eine zunehmende Durchdringung von Sensorik zu. Diese Entwicklungen zwingen dazu, dem Recht auf Anonymität Nachdruck zu verleihen. Dies erkennt der Koalitionsvertrag an: „*Das Recht auf Anonymität sowohl im öffentlichen Raum als auch im Internet ist zu gewährleisten*." (S. 109)

Damit ist verbunden, dass von anlassloser Überwachung Abstand zu nehmen ist und es überwachungsfreie Räume gibt. Dies betrifft insbesondere die Online-Welt: „*Allgemeine Überwachungspflichten, Maßnahmen zum Scannen privater Kommunikation und eine Identifizierungspflicht lehnen wir ab. Anonyme und pseudonyme Online-Nutzung werden wir wahren*" (S. 17f.). Diese Festlegung im Koalitionsvertrag widerspricht auch nicht einer Identifizierung oder der Verwendung von Klarnamen in Situationen, in denen dies – wie beispielsweise in Anwendungen des E-Governments – erforderlich oder von der betroffenen Person gewollt ist. Hier gilt es, auch für die europäische eID und im Miteinander der EU-Mitgliedstaaten auf datensparsame Nutzungsmöglichkeiten in der digitalen Welt hinzuwirken (zur Anonymisierung s. auch oben „Datennutzung und Datenschutz").

4.3 Schutz gegen IT-Schwachstellen

Die Neugewichtung der Sicherheit von Bürgerinnen und Bürgern sowie von Unternehmen und Behörden gegenüber den Methoden der Strafverfolgung und der Nachrichtendienste wirkt sich auch auf den Umgang mit erkannten Schwachstellen der IT-Sicherheit aus. „*Die Ausnutzung von Schwachstellen von IT-Systemen steht in einem hochproblematischen Spannungsverhältnis zur IT-Sicherheit und den Bürgerrechten. Der Staat wird daher keine Sicherheitslücken ankaufen oder offenhalten, sondern sich in einem Schwachstellenmanagement unter Federführung eines unabhängigeren Bundesamtes für Sicherheit in der Informationstechnik immer um die schnellstmögliche Schließung bemühen*" (S. 109). Auch in der schwierigen Abwägung zwischen der Schutzpflicht des Staates und dem Offenhalten von Möglichkeiten der Überwachung überwiegt die Erkenntnis, dass IT-Schwachstellen nicht nur der strafverfolgenden und nachrichtendienstlichen Tätigkeit nutzen, sondern auch vielen Kriminellen und Nachrichtendiensten anderer Staaten. Der Staat gefährdet durch die bisherige Praxis des Offenhaltens von IT-Schwachstellen die Rechte und Interessen, die zu schützen er verpflichtet ist.

Daher ist die Einrichtung eines Schwachstellenmanagements und die Neuausrichtung des BSI auf diese Aufgabe zu begrüßen. „*Wir leiten einen strukturellen Umbau der IT-Sicherheitsarchitektur ein, stellen das Bundesamt für Sicherheit in der Informationstechnik (BSI) unabhängiger auf und bauen es als zentrale Stelle im Bereich IT-Sicherheit aus. Wir verpflichten alle staatlichen Stellen, ihnen bekannte Sicherheitslücken beim BSI zu melden und sich regelmäßig einer externen Überprüfung ihrer IT-Systeme zu unterziehen. Das Identifizieren, Melden und Schließen von Sicherheitslücken in einem verantwortlichen Verfahren, z.B. in der IT-Sicherheitsforschung, soll legal durchführbar sein*" (S. 16).

Damit das BSI die ihm neu übertragenen Aufgaben auch effizient und ohne Zielkonflikte erfüllen kann, ist die Absicht der Koalition, das BSI unabhängiger aufzustellen, zu begrüßen. Denn es kann leichtv zu Zielkonflikten führen, wenn das BMI gleichzeitig die Fachaufsicht über das BSI sowie das BKA und den Bundesverfassungsschutz ausübt. Die Verpflichtung von staatlichen Stellen zu regelmäßigen Sicherheitsüberprüfungen ihrer IT-Systeme und zur Meldung von erkannten IT-Schachstellen an das BSI sollte ergänzt werden um Regelungen, wie die Hersteller von IT-Systemen und die Betreiber von IT-Diensten über IT-Schwachstellen ihrer Produkte und Dienste informiert werden. Auch sollten sie zur umgehenden Schließung von erkannten IT-Schwachstellen verpflichtet werden. „*Hersteller haften für Schäden, die fahrlässig durch IT-Sicherheitslücken in ihren Produkten verursacht werden*" (S. 16). Auch für private und professionelle Nutzer sollte der Umgang und das Melden von IT-Schwachstellen gegenüber BSI, Herstellern und Betreibern geregelt werden. Das Interesse an einer Meldung könnte durch eine Regelung zu einer angemessenen Belohnung (wie z.B. ein Finderlohn) unterstützt werden. Regelungen wie §§ 202a bis c StGB müssen überarbeitet werden, um

IT-Sicherheitsforschenden eine ausreichende Rechtssicherheit zu geben, dass Sicherheitsforschung zur Erhöhung der IT-Sicherheit auch an fremden IT-Systemen möglich ist.

5 ÜBERWACHUNG UND FREIHEITSSCHUTZ

„*Sicherheit und Freiheit bedingen einander*" (S. 6). An verschiedenen Stellen setzt sich der Koalitionsvertrag mit staatlichen Überwachungsmaßnahmen auseinander. So sollen eine Überwachungsgesamtrechnung eingeführt, die Vorratsdatenspeicherung rechtssicher ausgestaltet und der Einsatz von Überwachungssoftware beschränkt werden.

5.1 Überwachungsgesamtrechnung

„*Die Eingriffe des Staates in die bürgerlichen Freiheitsrechte müssen stets gut begründet und in ihrer Gesamtwirkung betrachtet werden. Die Sicherheitsgesetze wollen wir auf ihre tatsächlichen und rechtlichen Auswirkungen sowie auf ihre Effektivität hin evaluieren. Deshalb erstellen wir eine Überwachungsgesamtrechnung und bis spätestens Ende 2023 eine unabhängige wissenschaftliche Evaluation der Sicherheitsgesetze und ihrer Auswirkungen auf Freiheit und Demokratie im Lichte technischer Entwicklungen*." … „*Die Befugnis des Verfassungsschutzes zum Einsatz von Überwachungssoftware wird im Rahmen der Überwachungsgesamtrechnung überprüft*." (S. 108 f.)

Dias Gebot einer Gesamtbetrachtung aller staatlichen Überwachungsmaßnahmen lässt sich aus dem Urteil des BVerfG zur Vorratsdatenspeicherung herleiten. Danach darf die Freiheitswahrnehmung der Bürgerinnen und Bürgern nicht total erfasst werden und der Gesetzgeber muss bei Einführung neuer Überwachungsmaßnahmen die Gesamtheit der verschiedenen schon vorhandenen Datensammlungen im Blick behalten. Ein solcher Gesamtüberblick ist, nicht zuletzt aufgrund der zahlreichen und umfassenden Sicherheitsgesetze der letzten Jahre, eine gewaltige Aufgabe.

Aufgrund der reinen Masse an Überwachungsgesetzen ist schnelles Handeln gefordert. Es empfiehlt sich daher, zunächst den Blick auf den Bund als Gesetzgeber zu richten und einen pragmatischen, in der Praxis schnell einsatzfähigen Ansatz für eine Überwachungsgesamtrechnung zu finden. Dabei ist wichtig, dass objektive Bewertungskriterien für die Maßnahmen vorliegen. Allerdings ist zu beachten, dass pseudo-mathematische Berechnungen zu einer Schein-Objektivität führen und damit eine verlässliche Bewertung erschweren können.

Wichtig ist daher ein Kriterienkatalog, der dem Gesetzgeber Orientierung bietet. Dieser sollte Bewertungsmaßstäbe enthalten, um Eingriffe objektiv zu kategorisieren, und eine Systematisierung von Maßnahmen, die das Gewicht des Eingriffs abmildern können. Dieser Katalog kann mit der Zeit weiterentwickelt und auch für die Gesetzgebung in den Bundesländern übernommen werden.

„*Wir werden ein digitales Gesetzgebungsportal schaffen, über das einsehbar ist, in welcher Phase sich Vorhaben befinden. … Gesetzentwürfen der Bundesregierung wird künftig eine Synopse beigefügt, die die aktuelle Rechtslage den geplanten Änderungen gegenüberstellt*" (S. 10).

Die Erhöhung der Transparenz des Gesetzgebungsprozesses ist eine willkommene Verbesserung und kann es erleichtern, Gesetzesvorhaben schon frühzeitig in der breiten Öffentlichkeit zu diskutieren. Dies legt den Grundstein, um Transparenz über den gesamten Lebenszyklus von Gesetzen zu schaffen: durch Zugänglichkeit von Entwürfen, Nachverfolgbarkeit von Änderungen, eine unabhängige und qualifizierte Bewertung der mit einer Änderung verbundenen Auswirkungen – auch durch eine Überwachungsgesamtrechnung – bis zur Evaluation. Für die Evaluation von Gesetzen sollten zudem die gleichen Anforderungen gelten wie bei der Überwachungsgesamtrechnung. Sie sind von unabhängigen qualifizierten Stellen durchzuführen und es muss sichergestellt werden, dass die Kritik von Expertinnen und Experten nicht ignoriert, sondern konstruktiv aufgenommen wird.

5.2 Vorratsdatenspeicherung

„Angesichts der gegenwärtigen rechtlichen Unsicherheit, des bevorstehenden Urteils des Europäischen Gerichtshofs und der daraus resultierenden sicherheitspolitischen Herausforderungen werden wir die Regelungen zur Vorratsdatenspeicherung so ausgestalten, dass Daten rechtssicher anlassbezogen und durch richterlichen Beschluss gespeichert werden können." (S. 109)

In seiner ausführlichen Rechtsprechung zur Vorratsdatenspeicherung hat der EuGH u.a. in den Urteilen La Quadrature du Net und Privacy International festgelegt, dass diese nur anlassbezogen und aufgrund des damit verbundenen schweren Eingriffs grundsätzlich nur bei einer ernsten Bedrohung der nationalen Sicherheit und zur Bekämpfung von schwerer Kriminalität oder zur Verhütung ernster Bedrohungen für die öffentliche Sicherheit zulässig sind.

Soweit sich aus den gespeicherten Daten umfangreiche Persönlichkeitsprofile ableiten lassen, gelten generell erhöhte Anforderungen. Auch ist zu beachten, dass die Regelungen zeitlich auf das notwendige Maß zu beschränken sind, Datenschutzgarantien enthalten müssen, die Schutz vor Missbrauch bieten, und sicherstellen, dass die Speicherung keinen systematischen Charakter hat. Es ist nicht zu erwarten, dass der EuGH diese Maßstäbe im laufenden Verfahren gegen die deutschen Regelungen (verb. Rs. C-793/19 und C-194/19) substanziell abändern wird. Die bisher bestehenden deutschen Regelungen, die derzeit nur ausgesetzt sind, sind mit dieser Rechtsprechung nicht vereinbar und werden voraussichtlich vom EuGH für unvereinbar mit dem Europarecht erklärt, wie es der Generalanwalt bereits empfohlen hat.

Insofern verbleibt nur ein geringer Spielraum des Gesetzgebers für die Umsetzung einer Vorratsdatenspeicherung. Es ist als positiv zu werten, dass die Koalition sich gegen eine anlasslose Massenüberwachung ausgesprochen hat. Eine anlassbezogene Speicherung bestimmter Daten, die bereits unter den Stichwörtern Quick Freeze und Login-Falle diskutiert wurde und die keine Erstellung umfangreicher Persönlichkeitsprofile erlaubt, ist zur Bekämpfung und Verfolgung ernsthafter Kriminalität möglich. Dabei sind jedoch die Anforderungen, die EuGH und BVerfG bezüglich Schutzmaßnahmen aufgestellt haben, wirksam umzusetzen.

Angesichts dieser grundrechtlichen Beschränkungen ist eine Vorratsdatenspeicherung in der Form, wie sie bisher im TKG vorgesehen war, rechtlich nicht möglich. Daher ist Bundesjustizminister Buschmann zuzustimmen, dass die Vorratsdatenspeicherung „endgültig" aus dem TKG zu „streichen" ist (dpa vom 21.12.2021).

5.3 Beschränkung von Überwachungssoftware

„Für den Einsatz von Überwachungssoftware, auch kommerzieller, setzen wir die Eingriffsschwellen hoch und passen das geltende Recht so an, dass der Einsatz nur nach den Vorgaben des Bundesverfassungsgerichtes für die Online-Durchsuchung zulässig ist. … Das Bundespolizeigesetz novellieren wir ohne die Befugnis zur Quellen-TKÜ und Online-Durchsuchung. Solange der Schutz des Kernbereichs privater Lebensgestaltung nicht sichergestellt ist, muss ihr Einsatz unterbleiben. Transparenz und effektive Kontrolle durch Aufsichtsbehörden und Parlament werden wir sicherstellen." (S. 109)

In seinem Urteil zur Online-Durchsuchung hat das BVerfG das Recht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme, das sog. IT-Grundrecht, geschaffen. Aufgrund der großen Relevanz solcher Systeme für das Individuum im beruflichen und sozialen Alltag soll dieses Grundrecht verhindern, dass Dritte darin gespeicherte Daten ausspähen oder manipulieren können. Dies gilt insbesondere, da solche Vorgänge für das Individuum nicht stets erkennbar sind, sondern heimlich erfolgen können und auch Selbstschutzmaßnahmen nicht immer wirkungsvoll sind.

Daher dürfen Eingriffe durch den Staat nur zum Schutz vor konkreten Gefahren für ein überragend wichtiges Rechtsgut, wie Leib, Leben oder Freiheit einer Person oder den Bestand des Staates, erfolgen. Eine Online-Durchsuchung muss richterlich angeordnet sein und den Kernbereich privater Lebensgestaltung schützen. In diesen Kernbereich darf der Staat nicht eingreifen, da es Individuen möglich sein muss, ihre inneren Vorgänge höchstpersönlicher Art ohne Angst vor Überwachung auszudrücken. Daher muss zunächst verhindert werden, dass kernbereichsrelevante Sachverhalte überhaupt erfasst werden, und auf zweiter Stufe ist sicherzustellen, dass – soweit solche Inhalte dennoch erhoben wurden – diese umgehend gelöscht und nicht weitergegeben werden.

Da sich inzwischen umfassende Datenbestände aus sämtlichen Lebensbereichen auf Computern, Tablets und Handys von Individuen befinden, müssen jegliche Eingriffe, Zugriffe oder Veränderungen dieser Daten so transparent wie möglich erfolgen. Dies schließt bei heimlichen Maßnahmen insbesondere die nachträgliche Information betroffener Personen und Akteneinsicht ein, sobald keine Gefährdung des Ermittlungserfolgs mehr zu befürchten ist. Es ist weiterhin zu beachten, dass sich diese Daten nicht mehr nur auf den Endgeräten der Nutzenden befinden, sondern meist auch in der Cloud gespeichert werden. Daher müssen dieselben Anforderungen auch für Maßnahmen, die sich gegen Cloud-Anbieter richten, gelten.

Daneben ist der Staat aufgrund des Fernmeldegeheimnisses verpflichtet, die Kommunikation Privater zu schützen. Auch das IT-Grundrecht verpflichtet den Staat, zum Schutz der IT-Systeme von Nutzenden beizutragen. Bei Bekanntwerden ausnutzbarer Schutzlücken (insbesondere Zero-Day-Schwachstellen) besteht daher eine staatliche Schutzpflicht.

Insoweit ist der Gesetzgeber verpflichtet, eine gesetzliche Regelung zu treffen, inwieweit Sicherheitsbehörden solche Schwachstellen selbst ausnutzen dürfen, um die Systeme Verdächtiger zu infiltrieren. Diese Regelung muss die aufgrund einer Sicherheitslücke bestehende Gefahr für die Allgemeinheit und die Interessen der Sicherheitsbehörden abwägen.

Die Gefahr für die Allgemeinheit, die aufgrund von Sicherheitslücken besteht, hat sich wiederholt realisiert: So waren in den vergangenen Jahren immer wieder Krankenhäuser, Verwaltungen, Energieversorger und große wie kleine Unternehmen von Verschlüsselungstrojanern betroffen, die diese Zero-Day-Schwachstellen ausnutzen und teilweise monatelange Ausfälle in der Versorgung und dem Betrieb auslösten.

Hieraus müssen auch Anforderungen an die Förderung der Entwicklung und Kontrolle des Exports von Überwachungstechnologien folgen. Diese sind in den Ausführungen zur Rüstungskontrolle (S. 146) nicht eigens aufgezählt, können jedoch beim Einsatz durch repressive Regime ähnliche Wirkungen für die eigene Bevölkerung entfalten wie andere kontrollierte Rüstungsgüter.

5.4 Biometrische Überwachung und Social Scoring

„*Biometrische Erkennung im öffentlichen Raum sowie automatisierte staatliche Scoring Systeme durch KI sind europarechtlich auszuschließen*“ (S. 18).

Generell muss der Einsatz von algorithmischen Systemen, die mit einem zu großen Risiko für Individuen oder Gesellschaft verbunden sind, unterbunden werden. Es ist sinnvoll, dies auf europäischer Ebene zu adressieren und unionsrechtlich zu regeln, dass der Einsatz solcher Technologien wie biometrischer Erkennung im öffentlichen Raum und staatliches Scoring auf Basis von KI ausgeschlossen ist: Der Einsatz von Kameras mit Systemen zur biometrischen Identifizierung im öffentlichen Raum – sogar in Echtzeit – ist eine Technologie, die eine besonders intensive Form der Überwachung bedeutet, da sie eine detaillierte und umfassende Verhaltens- und Bewegungsprofilerstellung aller erfassten Personen ermöglicht. Sollten solche Systeme flächendeckend etwa an Verkehrsknotenpunkten eingesetzt werden, hätten selbst vermeintlich geringe Fehlerquoten erhebliche Auswirkungen auf den Alltag der falsch identifizierten Personen. Problematisch ist dabei, dass diese Systeme insbesondere bei bereits marginalisierten Gruppen, z.B. People of Color, eine besonders

hohe Fehlerquote aufweisen. Ähnliche Risiken bestehen beim Einsatz von algorithmischen Systeme, die als Künstliche Intelligenz (KI) bezeichnet werden. Ein staatlicher Einsatz – dem sich die Bürgerinnen und Bürger faktisch nicht entziehen könnten – mit dem Ziel eines Scorings ist abzulehnen. Auch wenn auf europäischer Ebene (noch) kein absoluter Ausschluss derartiger risikoreicher Verarbeitungen besteht, ist vom Einsatz abzusehen.

Zudem ist zu bedenken, dass nicht nur der Staat, sondern auch Privatunternehmen (wie beispielsweise Anbieter von sozialen Medien, Plattformen oder Cloud-Diensten) mit Hilfe der für sie verfügbaren personenbezogenen Daten zu einem Social Scoring in der Lage sein können. Daher wird ein Verbot jeglicher Art von automatisierter Bewertung des sozialen Verhaltens empfohlen.

Hinsichtlich der Ablehnung biometrischer Erkennung im öffentlichen Raum sowie automatisierter staatlicher Scoring-Systeme durch KI fokussiert die politische Debatte derzeit zu stark auf den Extremfall des automatisierten und flächendeckenden Einsatzes biometrischer Gesichtserkennung und staatlicher Scoring-Systeme. Zusätzlich müssen jedoch auch solche Verfahren diskutiert werden, die keine automatisierte flächendeckende biometrische Gesichtserkennung betreiben und trotzdem weitreichende Konsequenzen für die Grundrechte und Freiheiten der Bürgerinnen und Bürger haben. Hierzu zählen einerseits Systeme zur Erkennung und Interpretation von Verhalten und Emotionen, deren Wirksamkeit und Zuverlässigkeit wissenschaftlich höchst umstritten ist, wie sie für E-Recruiting, Personalführung, Gefahrenerkennung und Konsumentenbeeinflussung zu erwarten sind. Andererseits zählen hierzu prädiktive Risiko-Modelle, die mittels Nutzung von KI-Systemen Verhalten vorhersagen und so Diskriminierung ermöglichen. Zudem stammen derartige Systeme häufig von privatwirtschaftlichen Anbietern, sodass der Fokus auf staatliche Scoring-Systeme zu eng gefasst ist und um privatwirtschaftliche Anbieter erweitert werden sollte, sofern ein erhebliches und dem durch staatliche Stellen vergleichbares Risiko von der jeweiligen Verarbeitung ausgeht.

6 GESELLSCHAFTLICHER FORTSCHRITT DURCH DIGITALISIERUNG UND DATENSCHUTZ

Der Koalitionsvertrag enthält viele gute Ansätze, um gesellschaftlichen Fortschritt durch Digitalisierung und Datenschutz zusammen zu erreichen. Diese Ansätze sind nicht immer und überall im Vertrag auch ausreichend ausgeführt sowie mit geeigneten und effektiven Maßnahmen dargestellt. Dieses Policy Paper ergänzt die dargestellten Ansätze konstruktiv um konkretisierende und operative Zielsetzungen und um geeignete Vorschläge für hilfreiche Umsetzungsmaßnahmen. Diese positiven Ergänzungen sind an dem übergeordneten Ziel ausgerichtet, durch Verbesserung der Verwirklichungsbedingungen von Privatheit und Selbstbestimmung sozialnützliche und gesellschaftlich fortschrittliche 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 fortentwickelt, 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

ULD
Unabhängiges Landeszentrum für
Datenschutz Schleswig-Holstein