

Datenschutz und Digitalpolitik in krisenhaften Zeiten: eine Einleitung in den Band

Alexander Roßnagel, Michael Friedewald, Christian Geminn und Murat Karaboga

Wir leben in krisenhaften Zeiten – und diese gefährden Privatheit sowie individuelle und kollektive Selbstbestimmung. Krisenhafte Entwicklungen in der Geopolitik, in den Volkswirtschaften, in der Technologie, in der Sicherheit der Informationstechnik, in der inneren Sicherheit, in der öffentlichen Kommunikation und in weiteren gesellschaftlichen Bereichen verändern die Verwirklichungsbedingungen der Werte, die in der Europäischen Union das friedliche und gedeihliche Zusammenleben und Wirtschaften bestimmen sollen. Noch ist unklar, ob die damit verbundenen Herausforderungen die Werte selbst in Frage stellen, sie inhaltlich verändern oder nur ihre Umsetzung und Durchsetzung erschweren. Daher ist es von größter Bedeutung zu untersuchen, was auf dem Spiel steht, woher die Gefährdungen kommen und was man gegen sie unternehmen kann und soll.

Governance-Struktur europäischer Werte

Für die Gewährleistung europäischer Werte im Prozess der Digitalisierung ist eine Struktur entscheidend, die aus mehreren zusammenhängenden Elementen besteht: dem relevanten europäischen und auch mitgliedstaatlichen Rechtsrahmen, europäischen und mitgliedstaatlichen Institutionen für die Kontrolle und Durchsetzung des Rechtsrahmens, Adressaten, die die Vorgaben grundsätzlich akzeptieren, und politische Institutionen, die hinter diesen Werten stehen und bereit sind, den Rechtsrahmen positiv fortzuentwickeln. Gerät diese Governance-Struktur durch äußere oder innere Veränderungen unter Druck, kommt es für die Gewährleistung der Werte entscheidend darauf an, wie flexibel im Detail und wie stabil im Kern diese Governance-Struktur ist.

Die normativen Grundlagen für das gesellschaftliche Zusammenleben in Freiheit und Demokratie werden vor allem in der Europäischen Grundrechtecharta (GRCh) beschrieben. Auch in einer digitalen Welt soll die

europäische Gesellschaft geprägt sein von Menschenwürde, individueller und kollektiver Selbstbestimmung, Schutz vor Risiken und Rechtsstaatlichkeit. Der Prozess der Digitalisierung soll diese Werte nicht gefährden, sondern soll von ihnen geleitet werden. Er wird normativ einerseits von den Grundrechten auf Privatleben (Art. 7 GRCh) und Datenschutz (Art. 8 GRCh) und andererseits von den Grundrechten auf Meinungs- und Informationsfreiheit (Art. 11 GRCh), Forschungsfreiheit (Art. 13 GRCh), Berufsfreiheit (Art. 15 GRCh) sowie Unternehmensfreiheit (Art. 16 GRCh) geprägt. Bezogen auf die Verarbeitung personenbezogener Daten bietet die Datenschutz-Grundverordnung (DSGVO) auf einfachgesetzlicher Ebene einen Ausgleich zwischen diesen Grundrechten. Aus der Suche nach geeigneten Kompromissen enthält sie viele abstrakte technikneutrale Regelungen. Auch gibt sie den Mitgliedstaaten in vielen Öffnungsklauseln Möglichkeiten, jeweils ihre Vorstellungen von Datenschutz in nationalen Gesetzen – insbesondere für den öffentlichen Bereich – verbindlich zu machen.

Die Umsetzung dieses Rahmens für Ordnung und Entwicklung überlässt die Datenschutz-Grundverordnung in erster Linie den Datenverarbeitern, die sie „Verantwortliche“ nennt. Sie werden kontrolliert und beraten von unabhängigen Datenschutzaufsichtsbehörden. Diese koordinieren ihre Aufsichtspraxis im Europäischen Datenschutzausschuss. Den von der Datenverarbeitung betroffenen Personen stehen Informations- und Interventionsrechte zu. Sie können bei den Aufsichtsbehörden Beschwerde einlegen, wenn sie der Meinung sind, dass Verantwortliche gegen die Vorgaben der Datenschutz-Grundverordnung verstoßen. Diese wiederum können den Beschwerden mit Befugnissen zur Informationserhebung sowie Anordnungen und Sanktionen nachgehen.

Sowohl Verantwortliche als auch betroffene Personen können die Gerichte anrufen, wenn sie mit Entscheidungen der Aufsichtsbehörden nicht einverstanden sind. Die Gerichte prüfen diese Entscheidungen und legen offene Fragen dem Europäischen Gerichtshof zur unionsweit einheitlichen Entscheidung vor.

Auf diese Weise werden die normativen Regeln zum Schutz der Grundrechte im Prozess der Digitalisierung durch das Zusammenwirken von Verantwortlichen, betroffenen Personen, Datenschutzaufsichtsbehörden, Datenschutzausschuss, nationalen Gerichten und dem Europäischen Gerichtshof konkretisiert und umgesetzt.

Anpassungsfähigkeit

Diese Governance-Struktur bietet grundsätzlich einen elastischen Rahmen für die weitere Entwicklung der digitalen Gesellschaft. Sie bietet Innovationen der Informationstechnik und ihrer wirtschaftlichen Verwertung einen Freiraum und passt sich den dadurch entstehenden neuen Bedingungen durch angegliche Interpretation der normativen Vorgaben an. Zugleich wirkt sie auf Innovationen ein, sich innerhalb des angepassten normativen Rahmens zu halten.

Viele der technikneutralen normativen Vorgaben sind so abstrakt, dass ihre Anforderungen auch auf neue Technikentwicklungen, Geschäftsmodelle, Anwendungs- und Nutzungsformen übertragbar sind. Sie sind etwa im Bereich wirtschaftlicher Datenverarbeitung immer zulässig, wenn sie durch eine Einwilligung, durch einen Vertrag oder durch überwiegende berechnete Interessen gedeckt sind. Im Bereich öffentlicher Datenverarbeitung sind sie zulässig, wenn sie durch eine gesetzliche Regelung des Mitgliedstaats erlaubt werden. Begrenzt werden sie durch die ebenfalls sehr auslegungsfähigen Grundsätze der Zweckbindung, der Erforderlichkeit, der Datenrichtigkeit, der Transparenz und der Datensicherheit. Durch diese Konzeption können im Regelfall die innovativen Datenverarbeitungen zugelassen und zugleich die Rechte der betroffenen Personen geschützt werden. Probleme ergeben sich, wenn im öffentlichen Bereich eine gesetzliche Erlaubnis fehlt oder im Wirtschaftsbereich ein Erlaubnistatbestand für die Verarbeitung besonders schützenswerter Daten wie z.B. Gesundheitsdaten, biometrische Daten oder Daten zur ethnischen Herkunft oder politischen Meinung nicht greift.

Die innovative Auslegung der abstrakten Texte praktizieren die Verantwortlichen. Ob sie sich durchsetzt, hängt entscheidend von den Datenschutzaufsichtsbehörden und den Gerichten ab. Die Aufsichtsbehörden können unzulässige Datenverarbeitungen verhindern und sanktionieren. Verantwortliche und betroffene Personen können die jeweils zuständigen Gerichte anrufen. Zu innovativen Auslegungen wird es immer wieder zu Streitigkeiten kommen, deren Ergebnisse in der Union abschließend der Europäische Datenschutzausschuss und vor allem der Europäische Gerichtshof feststellen. Dabei haben die europäischen und nationalen Gesetzgeber formal immer die Möglichkeit, die normativen Texte ihren politischen Vorstellungen anzupassen.

Aber dieses System der flexiblen Reaktion auf Innovationen und andere Veränderungen seiner Verwirklichungsbedingungen kann an seine Grenzen

stoßen. Dies kann zum einen der Fall sein, wenn die neuen Herausforderungen zu groß und zu vielfältig werden und zu schnell aufeinander folgen. Dann können die Institutionen, die für eine Anpassung von Normativität und Innovation sowie für einen Ausgleich der Interessen der Datenverarbeiter und der betroffenen Personen zuständig sind, überfordert sein. Zum anderen können die Wirkungen der Veränderungen zu stark oder zu unübersichtlich oder die Differenzen zwischen der neuen Wirklichkeit und dem normativen Ziel zu gravierend sein. Dann können der Kern des Grundrechtsschutzes und die grundsätzlichen Möglichkeiten, eine praktische Konkordanz der konkurrierenden Grundrechte zu finden, betroffen sein. Dadurch kann eine Krise für die Gewährleistung entscheidender europäischer Werte entstehen.

Anzeichen für krisenhafte Entwicklungen

Jahrelang schien die Entwicklungsrichtung der europäischen Digitalpolitik klar: Angesichts der vielfältigen Herausforderungen würden die Europäische Union und Deutschland mit Regulierung vorangehen, um ihre Bürgerinnen und Bürger und die europäischen Werte zu schützen, gleichzeitig digitale Innovationen voranzutreiben und so die Europäische Union wieder zu einem ernstzunehmenden digitalen Akteur zu machen. Zahlreiche Digitalrechtsakte neben der Datenschutz-Grundverordnung – etwa zur Verantwortung für Digitale Dienste, zum Wettbewerb zwischen Digitalen Diensten, zur Datennutzung, zur Daten-Governance, zur Künstlichen Intelligenz und zum Europäischen Raum für Gesundheitsdaten – zeugen von dieser Politik.

Im Bereich des Datenschutzes hat sich seit der Verabschiedung der Datenschutz-Grundverordnung vor zehn Jahren die europäische Governance-Struktur weitgehend bewährt. Der Europäische Gerichtshof hat die Zahl seiner Entscheidungen zu Datenschutzfragen von durchschnittlich drei Entscheidungen pro Jahr vor 2020 auf 15 im Jahr 2022, 23 im Jahr 2023 und knapp 30 in den Jahren 2024 und 2025 gesteigert. Mit diesen Urteilen hat er viele praktisch relevante Fragen beantwortet und durch eine inzwischen gefestigte Rechtsprechung in diesen Fragen unionsweit Rechtssicherheit erreicht.

Der Europäische Datenschutzausschuss hat bis Juni 2026 in 121 Plenarsitzungen unzählige Beschlüsse gefasst und inzwischen 120 hilfreiche Leitlinien und 45 leitende andere Empfehlungen veröffentlicht, die zu einer

gleichartigen Auslegung und Anwendung der Datenschutz-Grundverordnung in der Union beitragen sollen. Sie werden durch Expert Subgroups des Europäischen Datenschutzausschusses vorbereitet, in denen nahezu alle Aufsichtsbehörden der Mitgliedsstaaten intensiv mitarbeiten.

In Deutschland hat die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder noch mehr Beschlüsse, Entschlüsse, Orientierungshilfen, Kurzpapiere und Anwendungshinweise verabschiedet, die eine bundesweit einheitliche Anwendung der Datenschutz-Grundverordnung ermöglichen. Diese unions- und deutschlandweite Zusammenarbeit der Aufsichtsbehörden hat sich eingespielt und funktioniert. Alle diese Ergebnisse zeugen von dem Bemühen der Aufsichtsbehörden, die Schutzversprechen auch im Alltag in allen Bereichen und Regionen umzusetzen.

Dennoch sind die Datenschutz-Grundverordnung, die beschriebene Governance-Struktur europäischer Werte und die europäische Digitalpolitik in jüngster Zeit unter Druck geraten. Zu viele und zu starke Herausforderungen wirken gleichzeitig auf sie ein. Zunehmend zeigen sich Anzeichen für krisenhafte Entwicklungen:

Geopolitische Herausforderungen

Datenschutz und Digitalpolitik in der Europäischen Union erfahren durch geopolitische Spannungen zunehmend Herausforderungen. Die Abhängigkeit Europas und Deutschlands in wichtigen Technikfeldern von anderen Volkswirtschaften hat sich im Bereich der Informationstechnik gravierend verstärkt und scheint sich weiter zu verstärken. Dies reicht von Rohstoffen und Hardware über Rechenzentren, Betriebssysteme und Cloud Computing bis hin zu vielen Ausprägungen der Anwendungssoftware. 9 von 10 Unternehmen in Deutschland sind hinsichtlich relevanter Informationstechnik und digitaler Dienste von außereuropäischen Anbietern abhängig.

Diese Abhängigkeiten führen zu Wettbewerbsnachteilen auf dem Weltmarkt ebenso wie auf dem heimischen Markt, bewirken durch Lock-in-Effekte Einschränkungen der wirtschaftlichen Entscheidungsfreiheit, führen zu Monopolisierungstendenzen, behindern Innovationen und erleichtern es, erfolgreiche europäische Start-ups aufzukaufen. Zugleich führt die Sammlung extrem großer Mengen personenbezogener Daten durch ausländische Konkurrenten und deren Zusammenführung zu Personenprofilen zu einer ungeheuren Machtsteigerung, da diese zur Steuerung individuel-

len und kollektiven Verhaltens nicht nur im Bereich der kommerziellen Werbung, sondern auch für politische Kommunikation verwendet werden können.

Mit der wirtschaftlichen Abhängigkeit steigt auch die politische und ökonomische Erpressbarkeit. Die gegenwärtige Regierung der USA mischt sich stärker als je eine amerikanische Regierung zuvor in die innenpolitischen Angelegenheiten europäischer Staaten ein und versucht, auf deren Entwicklung Einfluss zu nehmen. Dass sie nicht davor zurückschreckt, die technischen Abhängigkeiten von US-Software auszunutzen, zeigt die „Strafaktion“ gegen den Internationalen Strafgerichtshof in Den Haag und seine Mitarbeiter im Februar 2025. Diese Erpressbarkeit gefährdet die demokratische Willensbildung in Europa, die Anwendung europäischen Rechts und den Schutz der Grundrechte europäischer Bürgerinnen und Bürger.

Die Bemühungen um digitale Souveränität in der Union und in den Mitgliedstaaten nehmen zu, erleiden aber auch viele Rückschläge. Noch immer steigen die Umsätze der Unternehmen, die diese Abhängigkeit in Europa verursachen. Noch immer werden höhere Beträge an diese Unternehmen gezahlt, als in europäische IT-Angebote investiert und für europäische IT-Forschung ausgegeben. Die geopolitischen Herausforderungen und die damit verbundene krisenhafte Situation werden nur bewältigt werden können, wenn Politik, staatliche Stellen und Unternehmen in ihrer IT-Beschaffung massiv umsteuern, europäische Alternativen aufbauen und ihnen eine wirtschaftliche Durchsetzungschance geben. Ob der von der Europäischen Kommission im Juni 2026 vorgeschlagene Cloud and AI Development Act (CADA) einen Richtungswechsel hin zu mehr digitaler Souveränität bewirkt, wird sich zeigen.

Datenschutz als Wettbewerbsnachteil

Neben der Datenschutz-Grundverordnung hat die Europäische Union mit dem Digital Services Act und dem Digital Markets Act Regelungen getroffen, die für einen fairen Wettbewerb in der Union und für die Wahrnehmung von Verantwortung durch die Anbieter von sehr großen Plattformen sorgen sollen. Von diesen Plattformen sind viele andere Anbieter und nahezu alle Nutzerinnen und Nutzer digitaler Dienste abhängig. Obwohl diese Regelungen auch für ausländische Anbieter gelten, versuchen Anbieter aus den USA und China sich diesen europäischen Regelungen zu entziehen oder sie zu ignorieren.

Sie sammeln und teilen weiterhin personenbezogene Daten, die zur Verhaltensanalyse und -beeinflussung genutzt werden, und ignorieren dabei die Rechte der Nutzerinnen und Nutzer. Für deren Selbstbestimmung sind die Transparenz der Datenverarbeitung und die Möglichkeit individueller freier Entscheidung essentiell. Die Datenverarbeitung wird jedoch nur selten auf eine wirklich informierte Einwilligung gestützt. Ob es gegen diese Praktiken ausreichend ist, dass die Europäische Union mit einem Digital Fairness Act neue Instrumente gegen unfaire Praktiken der Internet-Werbeindustrie vorbereitet, ist zu bezweifeln.

Mit ihren Angeboten wenden sich große Plattformen auch gezielt an Kinder und Jugendliche und verarbeiten deren personenbezogene Daten. Dadurch ist aber nicht nur deren Datenschutz betroffen, sondern auch deren gesunde Entwicklung und der Schutz vor nicht kindgerechten Inhalten (z. B. Pornografie und Gewalt). Anforderungen an eine geeignete und datensparsame Altersverifikation und einen wirksamen Ausschluss von Minderjährigen von sie gefährdenden Angeboten werden weitgehend ignoriert.

Insbesondere im Datenschutz versuchen US-Konzerne ihre eigene Rechtsordnung, die weltweit gelten soll, zu ihren Gunsten in Form von Vertragsklauseln auch in Europa durchzusetzen. Sie wollen auf diese Weise ihre Angebote, auch wenn sie nicht datenschutzkonform sind, etablieren und dadurch ungerechtfertigte Marktvorteile erringen. Dafür nehmen sie auch immer wieder hohe Geldbußen der Europäischen Kommission und der Datenschutzaufsichtsbehörden in Kauf. Diese Praxis führt jedoch dazu, dass europäische Anbieter, die sich an die Vorgaben des europäischen Datenschutzrechts halten, Wettbewerbsnachteile erleiden.

Diese rechtliche Rahmung des Digitalsektors in Europa nimmt der amtierende US-Präsident immer wieder zum Ziel amerikanischer Handels- und Geopolitik. Er will damit europäische Regulierungen beeinflussen, die Anwendung ungeliebter rechtlicher Vorgaben verhindern und insbesondere Maßnahmen gegenüber US-Konzernen in Form von Bußgeldern und Wettbewerbsstrafen abwenden.

Dies stellt die Europäische Union und Deutschland einerseits vor die Frage, inwieweit sich bestehende Regelungen angesichts der Drohungen weiter gegenüber US-Konzernen durchsetzen lassen, und beeinflusst andererseits die Diskussion, wie die Digitalpolitik weiterentwickelt werden kann. Bezüglich der Durchsetzung bestehender Gesetze zeigen sich Organe der Europäischen Union bislang standfest. Es gibt aber auch andere Entwicklungen: So führen die in der KI-Omnibus-Verordnung 2026 fest-

gelegten zeitlichen Verschiebungen des Inkrafttretens der Verordnung für Künstliche Intelligenz (KI-VO) vor allem zu Vorteilen für US-Anbieter. Sie können sich bis dahin, ohne die Regeln der KI-VO einhalten zu müssen, auf dem europäischen Markt etablieren und entsprechende Abhängigkeiten begründen.

Technologische Entwicklung

Die europäische Digitalpolitik und insbesondere das europäische Modell, Datenschutz zu regeln und durch eine spezifische Governance-Struktur zu gewährleisten, geraten in jüngster Zeit durch die breite und rasante technologische Entwicklung unter Druck.

Die Datenschutz-Grundverordnung wurde vor inzwischen zehn Jahren verabschiedet. Sie baut auf der Europäischen Datenschutz-Richtlinie von 1995 auf und hat viele ihrer Regelungen übernommen. Sie beruht somit wesentlich auf Konzepten zur Gewährleistung informationeller Selbstbestimmung, die schon mehrere Jahrzehnte alt sind. Zwar haben die Unionsgesetzgeber versucht, den Einfluss der weiteren technologischen Entwicklung auf die Datenschutz-Grundverordnung dadurch zu begrenzen, dass sie ihre Regelungen so weit wie möglich technikneutral formuliert haben. Dennoch hatten sie unvermeidbar Vorstellungen von den zu regelnden Problemen, die ihrem Erfahrungshorizont mit Informationstechniken um 2016 und davor entsprachen. Daher liegen auch den angeblich technikneutralen Regelungen der Datenschutz-Grundverordnung unweigerlich Technikbilder aus der Zeit ihrer Entstehung zugrunde.

Neue Technologien, neue Geschäftsmodelle und neue gesellschaftliche Nutzungsformen verändern die Verwirklichungsbedingungen rechtlicher Regelungen. Aufgrund der beschriebenen Flexibilität der beschriebenen Governance-Struktur der Datenschutz-Grundverordnung muss nicht jede technische Änderung normativ oder durch Veränderung der Datenschutzpraxis nachvollzogen werden. Aber die neuesten Entwicklungen sind inzwischen so umfassend und gravierend, dass sie diese Flexibilität zu überfordern scheinen.

Ein wichtiges Beispiel hierfür ist die ubiquitäre Datenverarbeitung. Immer mehr alltägliche Geräte sind mit Datenverarbeitungskapazität und Kommunikationsfähigkeit ausgestattet, immer mehr Räume und Umgebungen, in denen Menschen sich aufhalten, sind mit Sensoren ausgestattet. Informationstechnik dringt in immer mehr Gesellschaftsbereiche, Ört-

lichkeiten und Handlungen ein und verändert soziale Praktiken in der Öffentlichkeit, der Familie und der Privatsphäre. Die Grenze zwischen datenschutzrechtlich irrelevanter privater Datenverarbeitung und relevanter Datenverarbeitung in der gesellschaftlichen Sphäre verschwimmt. Auf der einen Seite haben einzelne Personen – wörtlich genommen – in ihrer Hand eine größere Datenverarbeitungskapazität als vor wenigen Jahrzehnten ganze Rechenzentren und können damit ein größeres Datenschutzrisiko darstellen als früher große Datenverarbeiter. Auf der anderen Seite werden Smartphones und andere Techniken allgegenwärtiger Datenverarbeitung alltäglich von nahezu allen genutzt. Wo kann und muss gesellschaftliche Regulierung also ansetzen?

Allgegenwärtige Datenverarbeitung führt zu einer explosionsartigen Vermehrung personenbezogener Daten, die vielfältig genutzt werden. Sie ermöglichen tiefe Einblicke in Persönlichkeit und Beziehungen der betroffenen Personen. Dies ist die Grundlage für personalisierte Technikangebote und -nutzung. Personalisierung erleichtert technische Unterstützung erheblich, macht sie effektiver und angenehmer. Auf diese Weise können technische Assistenten ihre Nutzer in jeder Lebenslage unterstützen.

Personalisierung stellt jedoch zentrale Grundsätze des Datenschutzes in Frage – vor allem die Grundsätze der Zweckbindung und der Datenminimierung. Wenn ein persönlicher Assistent einen Nutzer in jeder Situation und bei jedem Problem unterstützen soll, kann seine Datenverarbeitung nicht auf einzelne Zwecke begrenzt sein. Sie muss vielmehr dem allgemeinen Zweck einer vollständigen und unvorhersehbaren Problembearbeitung dienen. Wenn der Assistent wissen soll, welche Ziele und Präferenzen sein Nutzer verfolgt und welche Bedingungen und Umstände er zu berücksichtigen hat, muss er alle Daten erheben, die für diese Aufgabe hilfreich sein können. Die Vorgabe, die Datenverarbeitung auf die wirklich erforderlichen Daten zu beschränken, führt zu keiner Einschränkung.

Herausforderungen bringt auch der Zeitaspekt. Die technologische Entwicklung erfolgt in immer kürzeren Innovationszyklen – meist schneller als die möglichen gesellschaftlichen Reaktionen. Diese erfordern wissenschaftliche Bewertungen, politische Diskurse und notwendige Verfahrensschritte der Gesetzgebung, der administrativen Behandlung oder gerichtlichen Beurteilung. Die technologische Entwicklung ist meist auch schneller als die Herausbildung adäquater sozialer und individueller Praktiken, wirtschaftlicher Anpassungen, der Erwerb neuer Kompetenzen und die Einrichtung neuer Ausbildungsgänge. Für den Datenschutz bedeutet dies: Soweit den immer neuen Herausforderungen nicht mit der Flexibilität der

Governance-Struktur europäischer Werte begegnet werden kann, wird die Diskrepanz zwischen den normativen Vorgaben der Datenschutz-Grundverordnung und ihrer operativen Umsetzung und den Herausforderungen für den Grundrechtsschutz immer größer.

Künstliche Intelligenz

Diese Herausforderungen zeigen sich vor allem bei der Künstlichen Intelligenz. Sowohl ihre Grundlagen wie auch ihre Anwendungen werden mit einer bisher ungewohnten Geschwindigkeit und in einer neuartigen gesellschaftlichen Tiefe und Breite entwickelt. In drei Jahren hat sie sich in allen Wirtschafts- und Verwaltungsbereichen ausgebreitet und wird in unterschiedlichsten Konstellationen – oft ungeordnet – genutzt.

Die Befürworter Künstlicher Intelligenz sehen vor allem die Chancen: Sie ist in vielfältigen Situationen zur Unterstützung und Übernahme von Arbeiten einsetzbar, nicht nur für Routinetätigkeiten, sondern auch für kreative Aufgaben. Sie verspricht Fortschritte in Wissenschaft und Medizin, Technologie und Kunst. Sie unterstützt Kommunikation und Kooperation und kann kommunikative Aufgaben bis hin zu emotionalen „Partnerschaften“ mit Menschen übernehmen. Künstliche Intelligenz kann Menschen in ihrer Selbstbestimmung stärken und in der Wahrnehmung anderer Grundrechte unterstützen, die Wettbewerbsfähigkeit von Unternehmen stärken und das Handeln von Verwaltungen effektivieren. Von vielen wird sie als *die* Grundlage für weiteren gesellschaftlichen Fortschritt angesehen.

Andere betonen die Risiken, die mit der Nutzung von Künstlicher Intelligenz verbunden sind: Sie verändert gesellschaftliche und wirtschaftliche Beziehungen tiefgreifend, indem sie Funktionen übernimmt, die bisher Menschen vorbehalten waren. Vor allem wird sie Arbeitsbeziehungen und Arbeitsbedingungen gravierend umgestalten – mit Auswirkungen auf Einzelne, Familien, gesellschaftliche Strukturen und Funktionen. Sie wird Lehren und Lernen inhaltlich wie prozessual auf neue Grundlagen stellen, Informationsgewinnung und -vermittlung beeinflussen sowie politische Prozesse und demokratische Willensbildung vor neue Herausforderungen stellen. Außerdem kann Künstliche Intelligenz missbraucht werden – zu Desinformation, Überwachung, Cyberangriffen und vielen weiteren unerwünschten oder unzulässigen Handlungen. Für viele bildet daher Künstliche Intelligenz die Grundlage für Befürchtungen über dystopische Entwicklungen der Gesellschaft, die nicht nur errungene und erkämpfte Werte

gefährden, sondern auch positive wertestärkende Entwicklungen verhindern.

So oder so – Künstliche Intelligenz verändert die Verwirklichungsbedingungen von Grundrechten und anderen Verfassungsprinzipien tiefgreifend – zum Guten oder zum Schlechten. Die Entscheidung darüber kann nicht einzelnen Konzernen überlassen werden. Ihre gesellschaftliche Steuerung und Gestaltung ist für eine lebenswerte Zukunft entscheidend.

Für die Governance-Struktur zur Gewährleistung der Grundrechte auf Privatleben und Datenschutz bedeutet Künstliche Intelligenz eine große Herausforderung ihrer normativen Grundlagen. Anbieter von KI-Systemen für allgemeine Anwendungen greifen weiterhin ungefragt auf personenbezogene und andere geschützte Daten zurück, um ihre KI-Modelle zu generieren. Ob und unter welchen Voraussetzungen KI-Systeme, die solche KI-Modelle nutzen, zulässig sind, ist weder geregelt noch geklärt. Die Datenschutzgrundsätze der Zweckbindung und der Minimierung personenbezogener Daten geraten bei Anwendungen Künstlicher Intelligenz noch stärker unter Druck als bei personalisierten IT-Anwendungen. Automatisierte Entscheidungen sind nach Art. 22 Abs. 1 DSGVO grundsätzlich unzulässig. Ob diese normative Festlegung aber angesichts der Fortschritte der – insbesondere agentischen – Künstlichen Intelligenz aufrechterhalten werden kann, ist eine offene Frage. Bisher können in vielen Sprachmodellen die Rechte betroffener Personen auf Berichtigung und Löschung von Daten nicht umgesetzt werden. Normative oder technische Lösungen für dieses Problem sind nicht ersichtlich.

In der Europäischen Union und in Deutschland wird eine große Diskussion darüber geführt, wie dem großen Vorsprung von USA und China in der Entwicklung von Künstlicher Intelligenz begegnet werden soll: Soll der Wettbewerb in der weiteren Verbesserung großer Sprachmodelle oder eher in der Entwicklung spezialisierter qualitativ hochwertiger KI-Systeme gesucht werden. Benötigt eine bessere Wettbewerbsfähigkeit einen möglichst großen regulatorischen Freiraum für die weitere ungestörte Entwicklung der Künstlichen Intelligenz oder soll sie mit der Ziel- und der Rahmensetzung erreicht werden, eine werteorientierte Künstliche Intelligenz zu entwickeln, die europäische Werte stärkt und nicht gefährdet?

Wirtschaftliche Krise

Nicht nur in der Entwicklung und Nutzung Künstlicher Intelligenz, sondern allgemein in vielen wirtschaftlichen Bereichen gilt die internationale Wettbewerbsfähigkeit Europas und Deutschlands mittlerweile als unzureichend. Insbesondere die Volkswirtschaft in Deutschland, die stark vom Export abhängig ist, leidet unter dem Rückgang von Exportquoten und niedrigem Wirtschaftswachstum besonders. Im Bereich digitaler Dienste herrscht sogar ein enormes Handelsungleichgewicht zwischen USA und Europa. Hierfür sind vor allem Verschiebungen in den Einflussmöglichkeiten auf die Weltwirtschaft zwischen USA, China, der Europäischen Union und sich entwickelnden Volkswirtschaften des Südens verantwortlich. Entscheidend sind auch die aktuellen Kriege und die Zollpolitik der USA.

Als ein zentrales Wettbewerbshindernis haben Vertreter der Wirtschaft und der Politik aber auch eine zu weitgehende Bürokratie ausgemacht. Sie drängen daher zu Lösungen, die sie vielfach in „Entbürokratisierung“ und dem Verzicht oder der Zurücknahme von Regulierungen im Digitalbereich sehen. Die Wettbewerbsbedingungen der deutschen Unternehmen sollen dadurch verbessert werden, dass sie von bürokratischen Pflichten entlastet werden.

Dies gilt auch für den Datenschutz, obschon bürokratische Belastungen durch Datenschutz nicht als das größte Problem angesehen werden. Gefordert werden Reformen der Datenschutz-Grundverordnung und des Bundesdatenschutzgesetzes. Die unterschiedlichen Vorschläge betreffen alle Ebenen der Governance-Struktur –sowohl die normativen Grundlagen mit den Regelungen zur Zulässigkeit der Datenverarbeitung, den Pflichten der verantwortlichen Datenverarbeiter und den Rechten der betroffenen Personen als auch die Zuständigkeiten in der Datenschutzaufsicht, die Zusammenarbeit der Aufsichtsbehörden und deren gesetzlichen Aufgaben und Befugnisse.

Zielsetzungen und abstrakte Maßnahmen zur Entbürokratisierung im Datenschutz haben CDU, CSU und SPD in ihrem Koalitionsvertrag vom 9. April 2025 formuliert, die bis Ende 2027 umgesetzt sein sollen. Vorschläge zur Änderung der Datenschutz-Grundverordnung hat die Europäische Kommission im Rahmen ihres Entwurfs für eine Digitale-Omnibus-Verordnung vom 19. November 2025 vorgelegt. Der Bundeskanzler und die Ministerpräsidentinnen und Ministerpräsidenten der Bundesländer haben am 4. Dezember 2025 eine gemeinsame Modernisierungsagenda beschlossen, die auch Vorschläge zur Reform im Datenschutz enthält.

Nicht jeder Vorschlag, dessen Umsetzung als Maßnahme der Entbürokratisierung gefordert wird, wirkt zielgenau und erreicht die gewünschte Wirkung. Werden die erwartbaren Wirkungen berücksichtigt, erweisen sich manche Vorschläge als Scheinentlastung, weil durch sie neue Rechtsunsicherheiten oder neue Handlungszwänge entstehen. Ein Beispiel ist die Aufhebung der Pflicht, ein Verfahrensverzeichnis zu führen. Dadurch entfällt zwar eine datenschutzrechtliche Verpflichtung, zugleich aber entfällt die Grundlage, viele andere Pflichten zu erfüllen, weil dies ein solches Verzeichnis faktisch voraussetzt.

Andere Vorschläge würden nur zu Belastungsverschiebungen führen, weil wenige Akteure von Belastungen befreit werden oder die Rechtssicherheit für sie verbessert wird, zugleich aber bei vielen anderen Akteuren neue Belastungen hervorgerufen werden. Beispielsweise käme die Übertragung der Datenschutzaufsicht in Bereichen der Wirtschaft von den Landesdatenschutzbeauftragten zum Bundesbeauftragten Verbänden oder sehr großen Verantwortlichen zu Gute, weil sie sich nur noch mit einer einzigen Verwaltungsstelle auseinandersetzen müssen. Diese Maßnahme würde aber kleine und mittlere Unternehmen (99 % aller Unternehmen) belasten, weil sie die Nähe zu ihrer gewohnten und regional vernetzten Aufsichtsbehörde und dem für sie zuständigen Gericht verlieren.

Schließlich wäre der Aufbau neuer Bürokratien keine geeignete Maßnahme zum Abbau von Bürokratie. Dies wäre aber notwendige Folge, wenn Zuständigkeiten der Landesdatenschutzbeauftragten zum Bundesdatenschutzbeauftragten verschoben würden. Ebenso bringt die Festlegung von Doppelzuständigkeiten für einheitliche Lebensvorgänge keine Entlastung, wie sie durch die Umsetzung des Data Act in Deutschland bewirkt wird: Nun sind in nahezu allen Fällen für den gleichen Lebenssachverhalt sowohl der Bundesdatenschutzbeauftragte als auch eine Landesdatenschutzbehörde zuständig.

Änderungen an der Governance-Struktur für den Datenschutz sollten sehr vorsichtig vorgenommen werden. Alle Vorschläge sind mit dem Versprechen verbunden, dass durch sie das Schutzniveau für Grundrechte nicht gesenkt werden soll. Viele Vorschläge bewirken jedoch genau dies. Daher sind die möglichen Folgen der Reformvorschläge sorgfältig daraufhin zu prüfen, ob sie tatsächlich unnötige Hemmnisse für die wirtschaftliche Entwicklung beseitigen, ob sie wirklich Erleichterungen für alle Unternehmen bieten, ob sie die Position der Unternehmen im Wettbewerb mit ausländischer Konkurrenz wirksam stärken und ob sie bei alledem zugleich effektiv einen Verlust an Grundrechtsschutz vermeiden.

Krisenhafte Zeiten

Die beispielhaft dargestellten Anzeichen für krisenhafte Entwicklungen wirken zusammen. Sie sind durch weitere – hier nicht erwähnte – Anzeichen zu ergänzen. Sie alle zusammen bewirken, dass die Gegenwart als krisenhaft erscheint. Bisherige Gewissheiten gehen verloren. Die Grundlagen, auf denen die Entwicklung von Wirtschaft und Gesellschaft bisher verlässlich aufbauen konnte, werden schwankend. Die krisenhaften Prozesse stellen die Governance-Struktur europäischer Werte, insbesondere der Werte der Privatheit und des Datenschutzes, vor Herausforderungen, die ihre inhärente Flexibilität und Anpassungsfähigkeit in Frage stellen. In der Folge verstärkt sich immer mehr der Druck, diese Governance-Struktur hinsichtlich materieller Inhalte, organisatorischer Institutionen und prozeduraler Abläufe zu verändern.

Hierfür ist aber eine Situation mit krisenhaften Einflüssen ein ungeeigneter Zeitpunkt: Die Zeit drängt, die Probleme sind kompliziert und komplex miteinander verwoben, die Maßnahmen müssen tiefgreifend sein, sind aber in ihren Auswirkungen schwer vorhersehbar. Für die notwendigen Reflexionen und Diskussionen, für die Bewertungen und Abwägungen fehlt es weitgehend an dem notwendigen Raum.

Der vorliegende Band versucht einzelne Aspekte, die das Krisenhafte an den gegenwärtigen Zeiten begründen, zu analysieren und zu bewerten. Soweit möglich, werden auch Aspekte möglicher Lösungen vorgestellt. Die Beiträge haben unterschiedliche Gegenstände und Perspektiven. Sie wählen bisweilen einen globalen Blick auf einen größeren Bereich, bisweilen gehen sie dem Krisenhaften in alltäglichen Lebenssituationen nach. Sie alle eint das Bemühen, dazu beizutragen, Auswege aus den jeweils angesprochenen Krisen zu finden.