Digitale Gesellschaft e. V.
Groninger Str. 7
D - 13347 Berlin

(030) 450 840 18

info@digitalegesellschaft.de
www.digitalegesellschaft.de

Berlin, Februar 2021

Digitalisierung politisch gestalten – Eckpunkte einer Agenda für die 20. Wahlperiode

Ein umfassendes Verständnis der Digitalisierung als zentraler Machtfrage des 21. Jahrhunderts ist eine Grundbedingung für politisches Handeln in den nächsten Jahren und Jahrzehnten.

Digitalisierung darf nicht rein technisch oder unter dem Blickwinkel einer bloßen wirtschaftlichen Standortpolitik betrachtet werden. Ihr emanzipatives Potential kann sie nur entfalten, wenn ihre Gestaltung den Grundrechten und den Bedürfnissen der gesamten Bevölkerung verpflichtet ist.

Nach Auffassung der Digitalen Gesellschaft sind ein freies Internet und die digitale Teilhabe Grundvoraussetzung einer offenen Gesellschaft im 21. Jahrhundert. Die politische Gestaltung der Digitalisierung muss auf dem Fundament der Rechtsstaatlichkeit aufbauen, den Grundrechten Geltung verschaffen und sich am Sozialstaatsprinzip messen lassen.

Als zentrale Themen, die die kommende Legislatur im Bereich der Digitalisierung prägen werden, haben wir die folgenden Punkte ausgemacht:

1. Digitale Infrastruktur – Open Source und ein sicheres Netz für die ganze Gesellschaft

Auch wenn im Laufe der kommenden Legislatur die Pandemie hoffentlich der Vergangenheit angehören wird, bleiben viele der durch sie aufgeworfenen Fragen ungelöst. Die plötzliche Umstellung weiter Teile von Wirtschaft und Gesellschaft in Homeoffice bzw. Homeschooling hat die massiven technischen Defizite in der öffentlichen Verwaltung und in weiten Teilen der Privatwirtschaft aufgezeigt. Eine veraltete Infrastruktur und unverhältnismäßig hohe Mobilfunkkosten erschweren großen Teilen der Bevölkerung die gesellschaftliche Teilhabe. Gerade im ländlichen Raum ist der Netzanschluss noch immer vollkommen unzureichend. Das Recht auf ein schnelles Internet ist daher ambitioniert und zeitnah umzusetzen.
Insbesondere der Mangel an einer technischen Infrastruktur, die ein sicheres und ansatzweise datenschutzkonformes Arbeiten unter den Pandemiebedingungen möglich macht, ist eklatant. Eine solche öffentliche Infrastruktur ist aber Grundvoraussetzung für ein demokratisches Gemeinwesen. Zu ihren wesentlichen Prinzipien gehören Open Source, Dezentralität, Verschlüsselung und Nachhaltigkeit. An ihnen ist eine umfassende Digitalisierungsstrategie auszurichten.

Open Source – Public Money? Public Code!

Bislang ist die öffentliche Hand noch in weiten Teilen von proprietärer Software mit restriktiven Lizenzen und ohne Zugriff auf den Quellcode abhängig. Das heißt, dass die Kontrolle weiter Teile der staatlichen und gesellschaftlichen Infrastruktur aus der Hand gegeben wird und durch Lock-in-Effekte ein Austausch mit anderen Systemen unnötig erschwert oder gar unmöglich gemacht wird. Auch die eigenständige Überprüfung der Sicherheit der verwendeten Systeme ist – wenn überhaupt – nur sehr erschwert möglich.

Wir fordern daher, die digitale öffentliche Infrastruktur auf der Grundlage freier Software zu modernisieren und es so öffentlichen Verwaltungen, Unternehmen und Individuen zu erlauben, öffentlich finanzierte Software frei zu verwenden, zu verstehen, zu verteilen und zu verbessern. Dies schützt öffentliche Verwaltungen davor, an die Dienstleistungen einzelner Hersteller gebunden zu sein, und stellt sicher, dass der Quellcode verfügbar ist, so dass Hintertüren und Sicherheitslücken unabhängig von einem einzigen Dienstleister geschlossen werden können.

Dazu bedarf es nicht nur der finanziellen Förderung einzelner Projekte und einer Vergabepolitik, die sicherstellt, dass Software, die öffentlich finanziert wird, als freie Software zugänglich ist. Neben dem Ausbau und der Förderung öffentlicher Forschungseinrichtungen, die an Open Source arbeiten, brauchen wir ein Stiftungswesen, das die unabhängige und gemeinwohlorientierte Entwicklung freier Software fördert. Wir schlagen daher die Schaffung eines europäischen ‚Open Technology Fund' sowie entsprechende Fördermöglichkeiten in der Bundesrepublik vor.

Eine dezentrale und widerstandsfähige Infrastruktur schaffen

Das Grundprinzip des Internets ist seine Dezentralität. Durch die Vermeidung zentralisierter Datenvorhaltung und -verarbeitung und zentraler Infrastrukturen wird das Netz sicherer und widerstandsfähiger gegen Ausfälle, Angriffe und Repressalien. Derzeit ist das Netz allerdings von einer zentralisierten Plattformökonomie geprägt, in der große Player nicht nur die Regeln vorgeben unter denen kommuniziert wird, sondern die auch die große Teile der technischen Infrastruktur bereitstellen und gigantische Datenmengen sammeln. Damit einher gehen nicht nur enorme Risiken für die individuellen Rechte von Nutzerinnen und Nutzern. Das freie Internet im Ganzen wird mehr und mehr in Frage gestellt – mit immensen ökonomischen und gesellschaftlichen Folgen, wie der Bildung von weltweiten Monopolen und der Konzentration von Informationsmacht bei diesen. Wir fordern von einer künftigen Regierungsmehrheit daher eine entschiedene Unterstützung und Förderung der Dezentralisierung und eines breiten Ökosystems von Betreibern digitaler Infrastruktur, um Abhängigkeiten von einzelnen Anbietern und großen Playern aufzulösen.

Durch Verschlüsselung Sicherheit gewährleisten

Grundlage einer sicheren Kommunikation im Internet ist eine funktionierende und effektive Verschlüsselung. Das Prinzip der Ende-zu-Ende-Verschlüsselung ist dabei alternativlos. Die erneuten und immer wiederkehrenden Versuche, diese im Namen einer vermeintlichen Sicherheit zu kompromittieren um Sicherheitsbehörden durch eine „Hintertür" Zugang zu verschlüsselter Kommunikation zu ermöglichen, sind nicht nur rechtsstaatlich bedenklich. Es gefährdet die sichere Kommunikation der gesamten Gesellschaft und Wirtschaft mit möglicherweise fatalen Folgen.
Schwachstellen und Sicherheitslücken in IT-Systemen, die dem Bundesamt für Sicherheit in der Informationstechnik und anderen Behörden bekannt werden, müssen umgehend geschlossen werden und dürfen nicht für polizeiliche und geheimdienstliche Zwecke ausgenutzt werden. Wenn derartige Sicherheitslücken nicht geschlossen werden, können sie ebenso von Kriminellen und fremden Behörden genutzt werden. Mittlerweile besteht ein großer Markt für derartige Schwachstellen, der in Deutschland bislang auch nicht unterbunden wird. Aufgabe der Sicherheitsbehörden ist es Gefahren zu bekämpfen, nicht sie für eigene Zwecke auszunutzen.
Das Recht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme ist ein zentrales Grundrecht in einer digitalisierten Gesellschaft und darf nicht durch den Staat untergraben werden. Der Rechtsstaat muss die tatsächliche Möglichkeit seiner Bürgerinnen und Bürger anerkennen miteinander zu kommunizieren, ohne dass Polizei oder Geheimdienste mithören oder -lesen können. Stattdessen muss die Verbreitung verschlüsselter Kommunikation gefördert werden und diese zum Standard erklärt werden.

Gegen Ressourcenverschwendung, für Nachhaltigkeit und ein Recht auf Reparatur

Der Lebenszyklus elektronischer Geräte ist oft überschaubar, nicht selten schließt schon das Produktdesign eine Reparatur aus. Die fortschreitende Digitalisierung führt dazu, dass viele Alltagsgeräte ohne die entsprechende – zumeist proprietäre – Software nicht zu reparieren sind. Große Hersteller nutzen ihre Marktmacht aus, Reparaturen zu monopolisieren oder zu unterbinden.
Hersteller sollten daher verpflichtet werden, Reparaturanleitungen, eventuell benötigtes Spezialwerkzeug und Ersatzteile auch für offene Werkstätten oder Privatpersonen langfristig bereitzustellen. Eine geplante Obsoleszenz, beispielsweise durch Einstellung des Supports oder nicht austauschbare Akkus ist nicht hinnehmbar. Hier gilt: Wird der Support beendet und werden keine Sicherheitsupdates mehr angeboten, muss der Quellcode als Open Source freigegeben werden.

2. Offenes Internet - Meinungsfreiheit und Zugang zu Informationen

Uploadfilter verbieten

Im Jahr 2019 wurde die Urheberrichtlinie trotz massiver und breiter Proteste gegen deren Artikel 17 von der EU beschlossen. Derzeit diskutiert die Bundesregierung einen Entwurf für die nationale Umsetzung der Richtlinie, der rund um die Einführung von Uploadfiltern gestrickt ist und deren Einsatz faktisch unumgänglich machen würde. Auch in anderen Bereichen droht der Einsatz, so etwa zur „Bekämpfung terroristischer Inhalte“. Uploadfilter aber stellen nicht nur eine massive Gefahr für die Meinungsfreiheit im Internet dar, sondern ihr umfassender Einsatz würde das offene und freie Internet insgesamt infrage stellen und eine Infrastruktur schaffen, die zur Kontrolle jeden missliebigen Inhaltes im Netz genutzt werden kann.
Auch wenn die Urheberrichtlinie noch in der laufenden Legislatur umgesetzt werden sollte, bleiben Uploadfilter auf der politischen Agenda. Die Schwierigkeiten der Umsetzung der Richtlinie verweisen auf die Grundproblematik des Artikel 17 der EU-Richtlinie, der sowohl eine allgemeine Überwachung aller Inhalte ausschließen will, zugleich aber eine umfassende Haftung vorsieht, wenn diese nicht erfolgt. Auf der Europäischen Ebene ist eine Korrektur für den grundlegend misslungenen Artikel 17 der Richtlinie unabdingbar. Eine künftige Regierung sollte ihren Einfluss im Rat geltend machen und auf eine Reform hinwirken, die den Einsatz von Uploadfiltern tatsächlich ausschließt. Eine günstige Gelegenheit hierzu bieten insbesondere die derzeit in der EU diskutierten Verordnungen zur Plattformregulierung.

Urheberrecht grundlegend reformieren

Die Diskussionen um Uploadfilter verweisen auf ein strukturelles Problem des Urheberrechts. Dieses ist verankert in einem anachronistischen Werkbegriff und auf analoge Vertriebssysteme ausgelegt, die von großen Medienunternehmen vehement verteidigt werden. Das bloße Übertragen des klassischen Urheberrechts auf das Internet schafft immer neue Probleme und dient lediglich zur Bewahrung überkommender Geschäftsmodelle einflussreicher wirtschaftlicher Akteure.
Statt das Internet den Anforderungen der Medienindustrie anzupassen, fordern wir ein Urheberrecht, das den Anforderungen moderner Kommunikation gerecht wird. Grundlage eines derartigen Urheberrechts wäre unter anderem ein Werkbegriff, der die Komplexität arbeitsteiliger kreativer Prozesse und analoger wie digitaler Kommunikationsformen anerkennt. Wir fordern daher als ersten Schritt eine umfassende wissenschaftliche Evaluation des bisherigen geltenden Urheberrechts und seiner gesellschaftlichen Funktion mit dem Ziel seiner umfassenden Novellierung.

Plattformen wirksam regulieren

Seit Jahren beobachten wir eine Zentralisierung des Internets bei einigen großen Internetkonzernen, die nicht nur immer weitere Bereiche der technischen Infrastruktur des Netzes kontrollieren, sondern auf deren Plattformen wie Facebook, Youtube oder Twitter ein Großteil der Kommunikation im Netz stattfindet. Eine Einhegung der Macht dieser Plattformen, die bislang die Regeln der Kommunikation weitgehend ohne gesellschaftliche Kontrolle diktieren können, ist daher längst überfällig. Eine solche Regulierung sollte den Einfluss, die Marktmacht und die problematischen Geschäftsmodelle der großen Internetkonzerne beschränken und nicht auf Kosten der Nutzerinnen und Nutzer gehen.

Auf europäischer Ebene: Digital Services Act gestalten

Derzeit werden auf europäischer Ebene die Verordnungsentwürfe der Kommission zu einer Regulierung der Plattformdienste, das „Digitale Dienste Gesetz“ und das „Digitale Märkte Gesetz“ diskutiert. Die zukünftige Bundesregierung hat über seine wichtige Rolle im Rat der Europäischen Union einen großen Einfluss auf diese Gesetzgebung. Wir erwarten, dass sie diesen Einfluss nutzt, um die dringend notwendigen Rahmenbedingungen für eine plattformbasierte Netzökonomie zu schaffen. Dabei sollten die Fehler des NetzDG ebenso wenig wiederholt werden, wie die Schwierigkeiten bei der Rechtsdurchsetzung der DSGVO. Zentrale Eckpunkte einer solchen Regulierung sind:

- Ausschluss von Uploadfiltern
Uploadfilter dürfen nicht im Laufe des Gesetzgebungsprozesses ihren Weg in die Verordnungen finden. Vielmehr muss sichergestellt werden, dass auch keine indirekten Anreize zu automatisierter Inhaltserkennung geschaffen werden. Mit der Umsetzung einer allgemeinen Plattformregulierung

besteht die Möglichkeit, einen Regulierungsmechanismus für Plattformen zu finden, der Fehlentwicklungen korrigieren kann und Uploadfilter auch in anderen Bereichen, etwa dem Urheberrecht, obsolet macht.

- Haftungsregeln
Die Haftungsfreiheit aus der E-Commerce-Richtlinie ist Grundlage für einen freien und offenen Austausch im Netz – nicht nur auf den großen Plattformen. Dieses Prinzip muss gewahrt bleiben. Eine allgemeine oder umfassende Überwachung darf weder vorgeschrieben, noch dürfen Anreize dazu gesetzt werden.

- Stärkung von Nutzerrechten
Es bedarf einer durchsetzbaren und sanktionsbewährten Verpflichtung zur klaren und verständlichen Kommunikation der Geschäftsbedingungen und ihrer Durchsetzung. Ein niedrigschwelliger Beschwerdemechanismus bei fehlerhafter Moderation ist ebenso notwendig wie die Möglichkeit zur Meldung rechtswidriger Inhalte und deren nichtautomatisierte Bearbeitung.

- Transparenz
Die Öffentlichkeit muss Einblick in die Algorithmen der großen Plattformen erhalten. Die Regeln, nach denen öffentliche Diskussionen geführt werden, müssen allgemein bekannt sein und dürfen nicht das Geschäftsgeheimnis privater Unternehmen bleiben.

- Rote Linien für personalisierte Werbung und Tracking
Personalisierte Werbung als Kern des Geschäftsmodells der Plattformen basiert auf der umfassenden Sammlung möglichst vieler persönlicher bis intimer Daten und der Erstellung detaillierter Profile der Nutzerinnen und Nutzer. Dieses Ausspionieren aller Nutzerinnen und Nutzer ist ebenso problematisch wie das Tracking zur Steuerung des Nutzungsverhaltens. Insbesondere bei deren Nutzung für politische Werbung, beim Tracking auf Medien- und Informationsangeboten und beim ‚real-time-bidding' sind klare rote Linien zu ziehen. Auch das Zusammenführen dieser Daten durch große Dienste, die neben Werbung auch andere Kerngeschäfte erbringen, gehört unterbunden.

- Effektive Durchsetzung
Zur Durchsetzung der Regulierung bedarf es einer unabhängigen europäischen Instanz, die über die nötige Ausstattung verfügt. Nur so kann verhindert werden, dass sich Plattformen durch die Wahl ihrer Niederlassung eine ihnen gewogene oder unzureichend ausgestattete Aufsichtsbehörde selbst aussuchen können.

In Deutschland: Rechte Gewalt wirksam bekämpfen, NetzDG ersetzen

Um die offene und freie Gesellschaft zu verteidigen und Gewalt und Hass im Netz zu bekämpfen, müssen neben deren gesellschaftlichen Ursachen die problematischen Geschäftsmodelle der großen Plattformen in den Fokus genommen und nicht die Rechte der Nutzerinnen und Nutzer beschränkt werden. Durch die Einführung des NetzDG wurde eine gefährliche Infrastruktur für umfangreiche staatliche Eingriffe geschaffen, bei der zudem originär hoheitliche Aufgaben auf die Plattformbetreiber abgewälzt werden – etwa die Bewertung der Rechtmäßigkeit selbst bei komplexen Straftatbeständen wie der Beleidigung, der Billigung von Straftaten (§140 StGB) oder dem problematischen § 129 StGB („Bildung krimineller Vereinigungen").
Es ist daher kein Wunder, dass das deutsche NetzDG mittlerweile auch von autoritären Staaten als Blaupause für Internetregulierungen genutzt wird. In einer demokratischen Gesellschaft aber darf eben nicht jedes Mittel recht sein, die Feinde der Freiheit zu bekämpfen. Statt autoritärer Eingriffe in die Freiheit des Internets bedarf es daher einer ausgewogenen Regulierung der Geschäftsmodelle der großen Plattformen und einer gesamtgesellschaftlichen Strategie gegen rechte Gewalt und menschenverachtende Ideologien. Das NetzDG sollte abgeschafft und durch eine ausgewogene europäische Haftungsregelung im Rahmen des Digital Services Act ersetzt werden.

3. Datenschutz – Grundrechte stärken, Sicherheit gewährleisten

Datenschutz ist eine der zentralen Herausforderungen der Digitalisierung. Er liegt quer zu vielen anderen Herausforderungen wie Umweltschutz, Migration, sozialer Gerechtigkeit und der Zukunft von Demokratie und Rechtsstaatlichkeit.

Mit der DSGVO liegt grundsätzlich ein geeignetes gesetzliches Instrument zum Schutz der Grundrechte bei personenbezogener Datenverarbeitung vor. Doch leider stößt sie an Grenzen. Ihre Aufgabe erfüllen kann sie nur, wenn sie weiter entwickelt wird und ihre Regeln durch die zuständigen Behörden auch tatsächlich durchgesetzt werden. Insbesondere bedarf es dazu einer umfassenderen bereichsspezifischen Gesetzgebung im europäischen und nationalen Recht, in der die Grundsätze der DSGVO konkretisiert werden.

Beschäftigtendatenschutz gesetzlich regeln

Die Digitalisierung der Arbeitswelt schreitet seit Jahren voran. Zahlreiche Arbeitnehmerinnen und Arbeitnehmer arbeiten mit und an elektronischen Geräten und kaum ein industrieller Fertigungsschritt ist nicht schon weitgehend digitalisiert. Dies und die technischen Möglichkeiten moderner Personalverwaltung eröffnen umfassende Überwachungsmaßnahmen am Arbeitsplatz. Diese Überwachung von Beschäftigten gilt es zu verhindern, datenschutzrechtliche Standards müssen auch in der Arbeitswelt sichergestellt werden. Dazu bedarf es endlich einer gesetzlichen Regelung zum Beschäftigtendatenschutz, die neben einer Begrenzung der Überwachung von Beschäftigten und entsprechenden Beweisverwertungsverboten auch den Einsatz von KI und anderen neuen Technologien regelt. Das Mitbestimmungsrecht der Beschäftigten bei allen datenschutzrelevanten Fragen muss garantiert werden.

Digitalisierung des Gesundheitswesens neu starten

Gesundheitsdaten sind besonders sensible Daten, die eines umfassenden Schutzes bedürfen. Die gesetzlichen Regelungen und die Praxis im Gesundheitswesen werden dem bislang in keiner Weise gerecht.
Seit Beginn des Jahres sind die Krankenkassen verpflichtet, den Versicherten elektronische Patientenakten (ePA) anzubieten. Die Souveränität der Nutzerinnen und Nutzer über diese sensiblen Daten ist jedoch nicht ausreichend gewährleistet. Zudem bestehen ernsthafte Zweifel an der Sicherheit des Telematiksystems. Unter diesen Voraussetzungen kann die ePA ihrer versprochenen Funktion nicht gerecht werden und sollte umgehend gestoppt werden.
Nicht erst die Pandemie hat gezeigt, dass Gesundheitsdaten für die medizinische Forschung unverzichtbar sind. Ein differenzierter und starker Datenschutz sowie die Gewährleistung hoher Sicherheitsstandards und die weitestgehende Anonymisierung sind kein Hemmnis für die Forschung sondern deren notwendige Voraussetzung. Denn nur so kann das nötige gesellschaftliche Vertrauen geschaffen werden, dass die sensiblen Gesundheitsdaten nicht missbraucht werden. Patientinnen und Patienten müssen selbst darüber entscheiden können, zu welchen Forschungszwecken ihre Daten verwendet werden dürfen.
Bisherige Ansätze einer Digitalisierung im Gesundheitswesen haben Patientenschutz und datenschutzrechtliche Belange systematisch ausgeklammert. Berechtigte Einwände aus Ärztinnen- und Patientenschaft wurden ebenso ignoriert wie datenschutzrechtliche und zivilgesellschaftliche Interventionen. Stattdessen wurden gefährliche Entwicklungen ohne Not vorangetrieben. Es bedarf daher dringend eines sofortigen Moratoriums der Digitalisierung im Gesundheitswesen und ihrer umfassenden Neuausrichtung.

Informationelle Selbstbestimmung auch für Geflüchtete gewährleisten

Das Grundrecht auf informationelle Selbstbestimmung gilt auch für Geflüchtete. Dieses wurde in den letzten Jahren immer weiter eingeschränkt. Während auf europäischer Ebene nach den Plänen für eine Eurodac-Verordnung sogar die Fingerabdrücke von Sechsjährigen zentral gespeichert werden sollen und ein umfassendes Screening aller Schutzsuchender geplant ist, wird auch in der Bundesrepublik fahrlässig mit den persönlichen Daten Geflüchteter umgegangen. Das Ausländerzentralregister ist für Geflüchtete zu einem Instrument der Totalerfassung geworden, das den Zugriff auf nahezu sämtliche persönlichen Daten für zahlreiche Behörden vom Verfassungsschutz bis zum Jobcenter erlaubt. Für Asylentscheidungen werden mittlerweile die Mobiltelefone Schutzsuchender systematisch ausgelesen und analysiert.

Da Datenschutz ein Grundrecht ist, das gerade für Hilfsbedürftige von besonderer Bedeutung ist, fordern wir die umfassende Beschränkung der Speicherung und des Abrufs personenbezogener Daten auf ein Niveau, das dem rechtsstaatlichen Grundsatz der Verhältnismäßigkeit entspricht.

Hersteller auf Datenschutz verpflichten

Die Pflicht zum Datenschutz durch Technikgestaltung ist bereits auf der Ebene der Hersteller und Produkte gesetzlich zu verankern. Bislang sind Hersteller für die Einhaltung der datenschutzrechtlichen Standards nur sehr begrenzt verantwortlich. Die Grundsätze des Datenschutzes durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen müssen allerdings schon auf der Ebene des Produktdesigns gesetzlich verankert werden.
Gerade im Bereich des Internet-of-Things (IoT) sind die Sicherheitsstandards teilweise verheerend; oftmals bestehen nicht einmal ausreichende Updatemöglichkeiten und auch das Bewusstsein der Nutzerinnen und Nutzer über bestehende Gefahren ist wenig ausgeprägt. Wir schlagen daher vor, Hersteller derartiger Geräte gesetzlich in die Verantwortung zu nehmen und zu regelmäßigen Sicherheitsupdates zu verpflichten. Kommen sie einer solchen Verpflichtung nicht nach oder beenden ihren Support, müssen sie spätestens zu diesem Zeitpunkt ihre Quelltexte als Open Source veröffentlichen, um zumindest Dritten das Schreiben und Bereitstellen von Sicherheitsupdates zu ermöglichen.

Digitaler Verbraucherdatenschutz: Sicherheitsgurte statt Warnhinweise

Die bloße informierte Zustimmung bietet keinen ausreichenden Schutz für die Datenverarbeitung durch Digitalunternehmen. Zwischen Unternehmen und Nutzenden besteht ein großes Machtungleichgewicht, das nicht durch bessere Informationen auf Seiten der Nutzenden ausgeglichen werden kann. Wie es angesichts der Massenautomobilität im letzten Jahrhundert einer Gurtpflicht bedurfte, braucht es gesetzliche Mindeststandards für digitale Dienstleistungen. Der nationale und europäische Gesetzgeber sollten diese durch konkrete bereichsspezifische Regelungen etwa für den Bereich der personalisierten Werbung und Tracking sowie roten Linien für digitale Produkte im Vertragsrecht einziehen. Zur Regulierung von Werbung und Tracking im Netz sollte die künftige Bundesregierung im Zuge der Verabschiedung bzw. Novellierung der ePrivacy-Verordnung sowie der Verhandlung des Digital Services Act für einen Paradigmenwechsel im Datenschutz streiten: Die Verantwortung der Datenverarbeiter darf nicht länger den Betroffenen aufgebürdet werden.

4. Sicherheitspolitik – Eine Kehrtwende ist dringend nötig

Seit Jahren beobachten wir, dass die Politik auf neue Herausforderungen mit der Schaffung immer neuer Kompetenzen für die Sicherheitsbehörden und der Ausweitung des Strafrechts reagiert. Doch gerade auf die großen Herausforderungen durch die Ausbreitung eines neuen Autoritarismus muss eine offene Gesellschaft mit der entschiedenen Verteidigung und Ausweitung gesellschaftlicher Freiheiten und rechtsstaatlicher Garantien reagieren.

Moratorium für neue Sicherheitsgesetze

Angesichts der immer weiter gehenden Vorverlagerung von Eingriffsbefugnissen der Sicherheitsbehörden und der Entgrenzung des Strafrechts ist eine Neuausrichtung der Sicherheitspolitik dringend geboten. Derzeit wird allzu oft den medial lautstark vorgetragenen Forderungen von Polizeiverbänden reflexartig entsprochen. Die Liste der Entscheidungen der Verfassungsgerichte ist lang, in denen diese zu dem Schluss kommen, dass neue Sicherheitsmaßnahmen die rote Linie des gerade noch Verfassungsmäßigen überschritten haben. Diese Entwicklung muss aufgehalten werden. Denn mindestens genauso lang ist die Liste mit Maßnahmen, die im Sinne der Rechtsstaatlichkeit abgeschafft gehören: Von der Aufweichung des Trennungsgebots zwischen Polizei und Geheimdiensten über Staatstrojaner und dem Aufbau einer Hackerbehörde beim Innenministerium bis zum Registermodernisierungsgesetz – sie ließe sich fast endlos fortsetzen. Wir fordern daher ein umfassendes Moratorium auf den Gebieten der Sicherheits- und Kriminalpolitik und eine Entschlackung des Strafrechts sowie die rechtsstaatliche Begrenzung von Behördenkompetenzen.

Evaluation und Überwachungsgesamtrechnung durchführen

Das BVerfG hat bereits in einer Entscheidung zu strafrechtlichen Ermittlungsmethoden aus dem Jahr 2005 von additiven und kumulativen Grundrechtseingriffen gesprochen, die in ihrer gemeinsamen Wirkung analysiert werden müssten. Die gesetzgeberische Praxis kommt dem leider bislang nicht nach. Statt dessen werden immer neue Sicherheits- und Strafgesetze ohne breite gesellschaftliche Diskussionen im Schnellverfahren beschlossen. Sofern überhaupt eine Evaluation der bisherigen Rechtslage stattfindet, erschöpft sie sich zumeist in bloßer Aufzählung von Fallzahlen und der Einschätzung der Sicherheitsbehörden selbst. Eine ernsthafte Analyse der tatsächlichen Gefahrenlage und eine Gesamtevaluation der bestehenden Sicherheitsarchitektur findet nicht statt. Wir fordern daher vor jeder Verabschiedung von Gesetzen im Bereich des Sicherheitsrechts eine Überwachungsgesamtrechnung oder eine Freiheitsbestandsanalyse vorzunehmen.
Darüber hinaus fordern wir eine unabhängige und breit angelegte Analyse der gesamten Sicherheitsarchitektur unter dem wesentlichen Gesichtspunkt des Eingriffs in die Grundrechte.
In eine solche Analyse müssen zwingend die Perspektiven der Bürger und Bürgerinnen einbezogen und insbesondere diejenigen berücksichtigt werden, die von diesen Eingriffsbefugnissen und den vorgesehenen Maßnahmen in besonderer Weise betroffen sind. Auf einer derartigen Grundlage kann in einer breiten gesellschaftlichen Diskussion die Neuausrichtung einer rechtsstaatlichen Sicherheitspolitik unter dem Leitbild einer freien und offenen Gesellschaft in Angriff genommen werden.

5. Digitales Engagement – Die offene und demokratische Gesellschaft stärken

Digitales Ehrenamt fördern

Insbesondere das vergangene Jahr hat gezeigt, dass eine vielfältige und unabhängige digitale Zivilgesellschaft nicht nur längst ein wesentlicher, sondern auch ein notwendiger Bestandteil der Gesellschaft ist. Unter großem persönlichen Einsatz tragen zahlreiche Menschen dazu bei, eine digitale Infrastruktur aufzubauen, die auch in Krisenzeiten zumindest Teile des öffentlichen Lebens aufrecht erhalten kann.
Während die Internetwirtschaft von der durch die Pandemie bedingten Krise profitieren konnte, war die Arbeit für die Akteurinnen und Akteure der digitalen Zivilgesellschaft nur unter den äußerst erschwerten Bedingungen möglich, die auch den Rest der Gesellschaft getroffen haben. Die Schaffung und der Erhalt eines gemeinwohlorientierten digitalen Ökosystems braucht eine stabile organisatorische Grundlage. Derzeit mangelt es jedoch an finanzieller Unterstützung für Organisationen und Initiativen aus der digitalen Zivilgesellschaft. Es braucht neue Fördermechanismen, die den Aufbau nachhaltiger Strukturen unterstützen und nicht nur vermeintliche Innovation im Blick haben. Die Entwicklung von Open Source Software und freien IT-Infrastrukturen muss gemeinnützig im Sinne der Abgabenordnung werden.

Beteiligung ernst nehmen

Eine Digitalisierung, die das Gemeinwohl ins Zentrum stellt, lässt sich nur gemeinsam mit den Akteuren der digitalen Zivilgesellschaft verwirklichen. Hierfür muss sich die Politik noch weiter für Vorschläge aus der Gesellschaft öffnen und diese in die Politikgestaltung miteinbeziehen. Dazu braucht es die Anerkennung zivilgesellschaftlicher Expertise und ein klares Bekenntnis, deren Wissen und Kompetenzen zu nutzen.
Derzeit wird ihre Expertise leider oftmals lediglich im Rahmen der vorgesehenen Verbändebeteiligung formal abgefragt. Allzu oft wird eine effektive Beteiligung durch extrem kurze Fristen zur Stellungnahme für komplexe Gesetzgebungsverfahren unmöglich gemacht. Denn wenn es selbst großen Verbänden mit entsprechenden professionalisierten Strukturen schon schwer fallen dürfte, innerhalb von 28 Stunden zu einer komplexen Thematik wie dem IT-Sicherheitsgesetz 2.0 Stellung zu nehmen, ist dies für zivilgesellschaftliche Organisationen, die oftmals ehrenamtlich arbeiten, schlicht unmöglich.
Von einer künftigen Regierungsmehrheit erwarten wir, dass sie die demokratische Beteiligung an Gesetzgebungsverfahren ernst nimmt und zivilgesellschaftlichen Akteuren die tatsächliche Möglichkeit einräumt sich einzubringen. Dazu bedarf es nicht nur einer klaren Regelung für angemessene Fristen sondern einer Aufarbeitung des Gesetzgebungsmaterials (etwa in Form von Synopsen etc.) und einer umfassenden Transparenz im gesamten Verfahren.