Sitzung des Länderrats
Berlin, 9. April 2016

Beschluss: vorläufig

Datenschutz sichert die Ressource Freiheit

Informationelle Selbstbestimmung ist ein Grundrecht und essentiell, um die Privatsphäre und die Entfaltung jedes Menschen zu schützen und zu ermöglichen. Trotzdem wird gerade aus Reihen der Bundesregierung immer wieder der Datenschutz offen in Frage gestellt und ein vermeintlicher Gegensatz von Datenschutz und wirtschaftlicher Entwicklung konstruiert. Zudem wird der Schutz persönlicher Daten als Hemmnis einer guten Sicherheitspolitik dargestellt.

Dies erleben wir gerade dieser Tage. Das Schema ist ein altbekanntes: Ein grausamer terroristischer Anschlag führt leider nicht zu einer sachlichen Diskussion über rechtstaatliche Präventions- und Ermittlungsmöglichkeiten, sondern er wird vielmehr von manchen unverzüglich genutzt, um auf Kosten des Datenschutzes an der Sicherheitsschraube zu drehen und unseren Rechtsstaat konstituierende Freiheitsrechte offen in Frage zu stellen.
Wenn der für den Schutz unserer Verfassung zuständige Minister zu Protokoll gibt, dass Datenschutz schön sei, aber in
Krisenzeiten und darüber hinaus Sicherheit Vorrang habe, offenbart dies ein krudes Rechtsstaatsverständnis, dem wir uns als Grüne entschlossen entgegenstellen. Die Zusammenarbeit der Polizeien und Sicherheitsdienste in Europa gehört verstärkt und professionalisiert, insbesondere mit Blick auf konkrete Verdachts- und Risikoanlässe. Das ist zweifelsohne mit klaren rechtstaatlichen Standards möglich, und so muss es auch endlich entschieden angegangen werden.

Wer, um von eigenen Versäumnissen der letzten Monate abzulenken, nicht mehr zustande bringt, als Freiheits- und Grundrechte wie den Datenschutz offen in Frage zu stellen, hat nicht ansatzweise verstanden, worum es den
Terrorist*innen geht, nämlich darum, unsere Gesellschaft zu spalten und die Freiheit und Offenheit unserer Demokratien anzugreifen. Die Antwort auf Hass und Terror kann und darf daher niemals Demokratieabbau und Krieg, sondern nur noch mehr Rechtsstaatlichkeit, Entschlossenheit, Freiheit und Toleranz sein.

Der Datenschutz - in der digitalen Realität unserer von Algorithmen zunehmend geprägten Gesellschaft ein noch essentielleres Freiheitsrecht denn je - schützt den/die EinzelneN vor unternehmerischer und staatlicher Ausspähung. Ein Hindernis für eine effektive Sicherheitspolitik ist er, zumindest in demokratischen Rechtsstaaten, nicht. Stattdessen stellen verlässliche und hohe, einheitliche Datenschutzstandards die Voraussetzung für eine gute und akzeptierte Arbeit von Polizei und Sicherheitsbehörden dar. Es ist nötig, endlich die zielgerichtete Verfolgung von Terrorverdächtigen zu verbessern und dafür mehr Personal

bereitzustellen.

Die Bundesregierung hat noch immer nicht erkannt, dass anlasslose Datensammlungen, erhoben etwas im Rahmen von Vorratsdatenspeicherungen, durch Bankdatenabgleiche oder durch Flugpassagierüberwachungen, nicht dazu geführt haben, die Sicherheit vor Anschlägen zu erhöhen, im Gegenteil: Die Suche nach der Nadel im Heuhaufen, das ist eine bittere Erfahrung aus den Anschlägen von Paris und Brüssel, wird für die Ermittler*innen immer schwieriger, die Lage in einem Meer aus Information immer unübersichtlicher.

Längst haben höchste Gerichte dieser Praxis präventiver, unserer Rechtsordnung fremder, anlassloser Datenspeicherungen mit Hinweis auf deren Unvereinbarkeit mit geltenden Grundrechten eine klare Absage erteilt. So ist die Rechtsprechung längst zu einem Korrektiv einer grundrechtsgefährdenden weil oft unverhältnismäßig agierenden Gesetzgebung der Großen Koalition geworden. Dabei wäre es ihre originäre Aufgabe, den Grundrechtsschutz zu gewährleisten und angesichts der massiven Bedrohungen der informationellen Selbstbestimmung rechtliche Sicherungsmechanismen wie beispielsweise den Art. 10 GG auszubauen. Dies würde nicht nur zu einem höheren Grundrechtsschutz der Bürger*innen, sondern auch zu mehr Daten- und Rechtssicherheit für die Unternehmen führen.

Datenschutz made in Germany

Datenschutz und wirtschaftlicher Erfolg sind keineswegs Gegensätze. Datenschutz und Datensicherheit sind für die große Mehrheit der Unternehmen vielmehr von essentieller Bedeutung und eine Zukunftschance für hiesige Unternehmen, die auf ein großes Know-How von IT-Sicherheitslösungen made in Germany zurückgreifen können. Mit Ausnahme der wenigen internationalen Akteure, die mit unseren Daten unvorstellbar viel Geld verdienen, wird das Fehlen von Rechtssicherheit und Standards ganz überwiegend als Hemmnis der wirtschaftlichen Entwicklung wahrgenommen.

Mehr noch: Datenschutz und Datensicherheit können eine, das haben die letzten Monate eindrucksvoll gezeigt, sehr erfolgsversprechende Wirtschaftsstrategie sein. Selbst große US-Konzerne haben zuletzt die marktstrategische Bedeutung von IT-Sicherheit und dem Schutz persönlicher Daten erkannt. Sie verlegen ihre Rechenzentren auf den europäischen Kontinent und wehren sich öffentlichkeitswirksam gegen die staatliche angeordnete Entschlüsselung von Mobiltelefonen in den USA. Der Grund ist sehr einfach: Vertrauen ist nicht nur gut für die Akzeptanz neuer, digitaler Angebote, sondern auch gut für Geschäfte. Dieses Vertrauen besteht in den USA aufgrund der Enthüllungen Snowdens und Verpflichtungen aufgrund von intransparenten Entscheidungen von Geheimgerichten nicht mehr. In Deutschland gehören durchgehende Ende-zu-Ende-Verschlüsselung noch immer nicht zum Standard bei großen IT-Projekten. Hierfür haben wir uns als Grüne immer wieder eingesetzt und auf die Bedeutung vertraulicher Kommunikation hingewiesen. Einige Unternehmen haben die Bedeutung sicherer Verschlüsselungslösungen mittlerweile, anders als die Bundesregierung, erkannt und werben offensiv mit einer „Cloud made in Germany“. Diese Beispiele zeigen, dass wir in unserem Ringen nach mehr Datenschutz und Datensicherheit immer mehr Verbündete haben. Noch wichtiger ist die Erkenntnis, dass Deutschland und Europa tatsächlich relevante Standards setzen und diese zukünftig hoffentlich auch durchsetzen können. Wir sollten daher Datenschutz und Datensicherheit zu einem Markenkern unseres Wirtschaftsstandorts machen. Hierfür bedarf es neben einer Stärkung bestehender Aufsichtsstrukturen, einer größeren Unterstützung der wichtigen Arbeit der Verbraucherzentralen auch der Unabhängigkeit des noch immer dem Bundesinnenministerium unterstellten Bundesamt für Sicherheit in der Informationstechnik.

Zudem brauchen wir eine anpackende Umsetzung der EU-Datenschutzreform in bundesdeutsches Recht samt Nutzung bestehender Gestaltungsspielräume, beispielweise bezüglich eines effektiven Beschäftigtendatenschutzes. Hier liegt eine wahre Mammutaufgabe vor uns. Genauso müssen wir bestehende wettbewerbs-, kartell- und fusionsrechtliche Regelungen dahingehend weiterentwickeln, dass zukünftig die Rolle monopolartiger Anbieter mit extrem hohen Datenkonzentrationen stärker berücksichtig wird.

Wir treten weiterhin für hohe Datenschutzstandards beim Datenaustausch mit Drittstaaten ein, die auch tatsächlich als Rechte ausgestaltet sind. Unser Verständnis des Datenschutzes als Grundrecht muss auch in diesen Abkommen zum Ausdruck kommen. Das hat zuletzt der Europäische Gerichtshof in seinem Urteil zum „Safe Harbor"-Abkommen unmissverständlich klargemacht. Das Urteil war nicht nur wie bereits zuvor das Urteil zur EU-Vorratsdatenspeicherungs-Richtlinie eine weitere wichtige Grundsatzentscheidung. Das Urteil war auch eine schallende Ohrfeige für die Bundesregierung, die, trotzt des Umstandes, dass wir immer wieder vor genau dieser Entwicklung gewarnt haben, bis zuletzt an dem klar rechtswidrigen Abkommen festgehalten hat. Die nach dem Urteil des höchsten europäischen Gerichts entstandene Rechtssicherheit geht somit voll auf ihr Konto. Sollte das nun vorgelegte „Privacy Shield" erneut vom EuGH kassiert werden, hat sie die erneut entstehende Rechtsunsicherheit zu verantworten.

Mit Datenschutz schwarze Zahlen schreiben

Schon jetzt werden von europäischen Unternehmen mit Soft- und Hardware basierter Sicherheitstechnik Milliarden umgesetzt. Diese Technik dient auch dem Schutz der Daten der Verbraucherinnen und Verbraucher bei der Verwendung vernetzter Geräte und wird in diesem Sinne beworben. Wir sind überzeugt, dass wie bei den Umwelttechnologien auch Produkte, die Datenschutz und Datensicherheit in besonderer Weise gewährleisten, Exportschlager sein können. Das bedeutet, dass wir den Mittelstand in punkto IT-Sicherheit voranbringen und damit zukunftsfähig machen müssen. Auch Startups, die bewusst in entsprechende Lösungen investieren, müssen sehr viel stärker unterstützt werden als bisher.

Wir wollen die rechtlichen Rahmenbedingungen so gestalten, dass Verbraucher*innen in die Lage versetzt werden, bewusste Kaufentscheidungen zu treffen und so datenschutzkonforme und -sichere Produkte auszuwählen. Hierfür ist es von Nöten, mehr Transparenz, beispielsweise bezüglich eingesetzter Algorithmen, zu schaffen. Angelehnt an die Energieeffizienzklassen von Haushaltsgeräten soll eine entsprechende Klassifizierung oder auch Zertifizierung für vernetzte Haushaltsgeräte, Fahrzeuge etc. eingeführt werden.

Das Recht auf Verschlüsselung sowie ein Recht auf Anonymisierung ohne Hintertüren muss dauerhaft gesichert und ausgebaut werden. Diese Standortvorteile gegenüber den USA gilt es zu bewahren und festzuschreiben, auch und gerade gegenüber staatlichen Stellen. Klare Zugriffsbeschränkungen deutscher Nachrichtendienste sind zwingend eindeutig zu definieren und effektiv zu kontrollieren. Wir setzen uns zudem für eine verfassungsrechtliche Einhegung der Befugnisse der Dienste sowie eine komplette Neuaufstellung der Aufsicht geheimdienstlicher Tätigkeit ein.

Wir halten zudem ein staatlich finanziertes Programm zur Beratung bei der IT-Sicherheit für kleinere und mittlere Unternehmen (KMUs) für notwendig. Auch hier bieten die Erfahrungen des Umweltschutzes mit der Energieberatung gute Anknüpfungspunkte für die weitere Ausgestaltung. Sicherheitsberatung in die Fläche zu bringen, erhöht nicht nur den Schutz für die Unternehmen, sondern schützt vor allem die Daten der Millionen Kund*innen, die bei diesen

Unternehmen vorliegen. Mit diesem dezentralen Netz an IT-Sicherheitsberater*innen kann auch eine erste Aufklärung über Digitalisierung, Automatisierung und Vernetzung in den KMUs stattfinden, und damit das notwendige Umdenken und Überdenken anstoßen.

Datenschutz ist der neue Umweltschutz

Neben einer lebenslang vermittelten Medienkompetenz, sind Datensouveränität und Datensicherheit heute wesentliche Bedingungen für ein freies und selbstbestimmtes Leben. Je mehr der Staat oder Unternehmen über mich wissen, desto unfreier werde ich. Ich verhalte mich anders, wenn ich weiß, dass ich beobachtet werde und Spuren hinterlasse, über die ich keine Kontrolle mehr habe. In einer solchen Situation passen wir uns alle an. Die Schere im Kopf entsteht. Das ist Gift für die Demokratie. Freiheitliche Gesellschaften brauchen Freiräume, in den sich die Bürger*innen unbeobachtet ausprobieren und entfalten können. Es ist nicht nur für jeden schön, auch Geheimnisse haben zu können - für bestimmte Gruppen wie Journalist*innen, Ärzt*innen, Rechtsanwält*innen und Seelsorger*innen ist es sogar essentiell. Eine geschützte Kommunikation muss daher nicht nur ihnen zwingend ermöglicht und ausgebaut werden.

Der Staat und einige Unternehmen betreiben daher mit ihrer Datensammelwut Raubbau an der Ressource Freiheit. Und wie beim Umweltschutz können wir Fehlentwicklungen im Nachhinein nicht oder nur mit sehr viel größeren Aufwand reparieren. Der „Point-of-no-return“, die digitale 2-Grad-Grenze naht: Denn wenn meine Daten erst einmal in den Datenbanken großer Unternehmen und (fremder) Staaten gespeichert, gerastert und zu höchst aussagekräftigen Profilen verknüpft sind, haben wir die Kontrolle hierüber bereits verloren. Daher müssen wir jetzt handeln und den immer weiter ausufernden Datensammlungen und einer weitreichenden Spionage klare rechtliche Grenzen setzen. Die Politik darf den technischen Möglichkeiten und den durch sie entstehenden Gefahren für den Grundrechtsschutz nicht länger hinterherlaufen, sondern muss die Digitalisierung und den Schutz privater Kommunikation und Geschäftsgeheimnissen als vordringliche Herausforderung annehmen.

Als Bürgerrechtspartei liegt es auch in der besonderen Verantwortung der Grünen, die Bedeutung eines innovativen Datenschutzes als Grundlage für ein selbstbestimmtes Leben auch und gerade in der digitalen Welt immer wieder zu betonen.

Grundrechte in der digitalen Welt stärken

Wie nötig aber auch der Ausbau bestehender Mechanismen zum Schutz vor unternehmerischer und geheimdienstlicher Ausspähung ist, halten uns anhaltende Datenskandale, IT-Angriffe auf den Deutschen Bundestag und andere Institutionen und nicht zuletzt die anhaltenden Enthüllungen des Whistleblowers Edward Snowden vor Augen.

Der Datenschutz ist es, der einem totalitären Anspruch datensammelnder Unternehmen und Geheimdienste einen Riegel vorschiebt und verhindert, dass auch der letzte Teil unserer Privatsphäre verdatet wird. Er verhindert, dass unser aller Leben bis in den letzten Winkel überwacht, gerastert und profiliert wird. Längst geht es nicht mehr um einzelne Datensätze, sondern um die Zusammenführung und systematische Analyse aller vorhandenen Daten und Informationen. Aktuell befinden sich diese Daten oftmals noch verteilt in unterschiedlichen Datenbanken rund um den Globus. Immer öfter werden sie jedoch von Unternehmen verknüpft und gerastert. Und staatliche Stellen, das ist die Erkenntnis nach gut zwei Jahren Aufklärung im Untersuchungsausschuss des Bundestags zur geheimdienstlichen Praxis von NSA und BND, verschaffen sich auf legalem oder illegalem Weg Zugriff auf sie.

Die skizzierten technologischen Entwicklungen werden uns absehbar auch die kommenden Jahrzehnte begleiten. Die digitalen Datenmengen, die wir produzieren, verdoppeln sich in immer kürzeren Intervallen. Und mit ihnen steigen auch die Begehrlichkeiten, an diese Datenberge heranzukommen, sie zu vermarkten, zu rastern, zu Profilen zu verknüpfen und uns alle in ein digitales Kastensystem einzusortieren, das im offenen und klaren Widerspruch zu bestehenden Solidarsystemen steht.

Als Grüne werden wir nicht müde auf diese Gefahren für die informationelle Selbstbestimmung der Menschen hinzuweisen. Wir werden nicht müde, die Bundesregierung aufzufordern, sich, statt den Datenschutz in Frage zu stellen, auch endlich an den für die digitale Gesellschaft so wichtigen Fragestellungen angemessen zu beteiligen.

Auch die Bundesregierung muss sich fragen, ob bestimmte Geschäftsmodelle mit der Menschenwürde vereinbar sind, und ob es nicht Grenzen der Überwachung und Ausforschung, und der Algorithmisierung ganzer Lebensbereiche geben muss. Darüber, ob man monopolartige Anbieter und Plattformen mit extremen Datenanhäufungen nicht zwingen muss, ihre Algorithmen ganz oder teilweise offenzulegen, damit Aufsichtsbehörden zumindest eine gewisse Vorstellung davon bekommen können, welche Daten nach welchen Kriterien zu Profilen verknüpft an Dritte weiterverkauft werden und ob das bestehende Wettbewerbs- und Kartellrecht nicht angesichts extremer Datenanhäufungen bei wenigen großen Unternehmen angepasst und fit für das digitale Zeitalter gemacht werden muss.

Bislang ist der Druck auf die Bundesregierung, sich Überwachung und Ausforschung entgegenzustellen, nicht sonderlich groß. Das wird sich jedoch ändern: Die tatsächlichen Auswirkungen der derzeit stattfindenden, allumfassenden Vermessung unseres Lebens werden viele Menschen erst später spüren, dann aber in voller Härte: Aufgrund der falschen Wohnlage oder Freunde werden sie keine Kredite und keine Versicherungen mehr bekommen. Ihnen wird die Einreise in Länder verwehrt werden, weil ein Analyseprogramm die Ironie, die in einem privaten Online-Chat verwendet wurde, nicht erkannt und sie als potentielle Gefährder*innen charakterisiert hat, und sie werden erleben, wie ihr eigenes Auto vor Gericht gegen sie aussagt.

Die Bundesregierung beschäftigt sich mit all diesen Fragen bislang nicht, weil sie weiß, dass sie selbst höchst ambivalent agiert: Unternehmen verpflichtet man im Rahmen der anlasslosen Vorratsdatenspeicherung, die sich gegen 80 Millionen Bürger*innen richtet, neue Datenberge mit hoch sensiblen Kommunikationsverbindungsdaten anzuhäufen.

Während man Deutschland zum „Verschlüsselungsstandort Nummer eins“ auf der Welt machen will, sinniert man gleichzeitig über das Verbauen von permanenten Hintertüren in Hard- und Software, die immer auch Kriminellen offenstehen und betätigt sich als Hehler von Sicherheitslücken auf dem Schwarzmarkt. Hierdurch gefährdet man die IT-Sicherheit und die Privatheit von Kommunikation massiv. Sämtliche unserer Vorschläge, beispielsweise durchgehende Ende-zu-Ende-Verschlüsselungen in alle IT-Großprojekte einzuziehen, hat die Bundesregierung bislang stets abgelehnt. Das rächt sich heute, in Zeiten, in denen entsprechende Angebote echte Exportschlager wären.

Obwohl bis heute der verfassungskonforme Einsatz von in privateste Lebensbereiche vordringenden „Staatstrojaner“ zur Infiltrierung computertechnischer Systeme nicht nachgewiesen werden konnte, hält die Bundesregierung an diesem grundrechtlich hoch umstrittenen Instrument fest und greift noch immer auf das Know-How höchst zweifelhafter

Firmen zurück, die eine Prüfung der Verfassungskonformität durch Einblick in den Quellcode der Software mit Hinweis auf Betriebs- und Geschäftsgeheimnisse verwehren und ihre mit deutschem Steuergeld gebaute Technik - durch das Verrücken eines Kommas im Quellcode aufgetunt - in aller Despotenhände dieser Welt exportieren und dabei helfen, oppositionellen Protest im Keim zu ersticken und Menschen in Folterkeller zu verbringen.

Der sich aus dem Grundgesetz abzuleitenden Verpflichtung, unsere digitale Infrastrukturen und private Kommunikation effektiv zu schützen, kommt die Bundesregierung bis heute nicht nach. Bei der EU-Datenschutzreform hat sie eine unrühmliche Rolle gespielt und die so wichtige Reform, die einen Meilenstein für den Grundrechtsschutz von mehr als 500 Millionen Europäer*innen darstellt, über Jahre ausgebremst und auch hier grundlegende, unseren Rechtsstaat konstituierende Datenschutzprinzipien wiederholt offen in Frage gestellt.

Wichtige Verbündete für uns sind und bleiben die Datenschutzbeauftragten der Länder und des Bundes sowie die Verbraucherschutzverbände. Sie nehmen auch schon jetzt eine hervorgehobene und wichtige Rolle im Datenschutz ein. Eine weitere auch institutionelle Stärkung, so dass jede oder jeder Datenschutzbeauftragte weisungsfrei die eigenen Aufgaben erfüllen kann, ist unser Ziel. Wie Grüne stellen sicher, dass die Datenschutzbeauftragt*innen ihrer Rolle auch gerecht werden können. Das ist gerade etwa mit Blick auf die von der EU geschlossenen Abkommen zum Datenaustausch bisher nicht der Fall. Wir fordern daher, den Datenschutzaufsichtsbehörden von Bund und Ländern entsprechend den Vorgaben aus dem Urteil des EuGH vom 6. Oktober 2015 ein normiertes Klagerecht einzuräumen.

Transparenz ausbauen und Hass und Hetze bekämpfen

Wir wollen die Chancen der Digitalisierung für die Gesellschaft und die staatlichen Prozesse noch besser nutzen, unsere Demokratie vitalisieren, das Verhältnis von Bürger*innen und Staat reformieren und die Legitimität politischer Entscheidungen erhöhen.

Ein besonders positives Beispiel sind die Transparenzgesetze einiger Bundesländer, die die Verwaltung verpflichten, eine Vielzahl von Dokumenten und Daten kostenfrei und online zur Verfügung zu stellen. Hier sind insbesondere Hamburg und Rheinland-Pfalz derzeit an der Spitze. Private Daten werden in dem Verfahren geschützt, in dem das Informationsregister grundsätzlich keine personenbezogenen Daten enthalten darf. Ein Transparenzgesetz in diesem Sinne stärkt die demokratische Teilhabe und das Vertrauen in staatliche Entscheidungsprozesse. Wir wollen nicht nur auf Bundesebene ein umfassendes Transparenzgesetz, sondern auch in den Bundesländern, in denen es solche Gesetze bislang noch nicht gibt und ermutigen alle, daran aktiv mitzuwirken.

Die Pläne des Staates gehen häufig über die bloße Bereitstellung von Informationen hinaus. Viele Verwaltungsangebote sollen zunehmend online erfolgen. Auch Wirtschaft, Verkehrssysteme sowie Bildungsnetzwerke sollen weiter digitalisiert werden. Die enormen Entwicklungspotentiale wollen wir nutzen. Allerdings sind Datenschutz und Datensicherheit notwendige Voraussetzung für Vertrauen in diese neuen digitalen Angebote. Nur dann werden die Bürger*innen die Vorteile der Digitalisierung langfristig annehmen und entsprechende Angebote unbeschwert nutzen. Das bedeutet, Verfahren und Geschäftsprozesse müssen von Beginn an so konzipiert, strategisch angeleitet, umgesetzt und praktiziert werden, dass sie der informationellen Selbstbestimmung und der Vertraulichkeit und Integrität informationstechnischer Systeme Rechnung tragen. Prinzipien des Datenschutzes, der Informationsfreiheit und -sicherheit wie etwa der Gesetzesvorbehalt, die Erforderlichkeit,

die Datenerhebung bei Betroffenen, Privacy by Design und Default, die Zweckbindung der Daten, Datenvermeidung und -sparsamkeit, Schutzbedarfsfeststellung und Risikoanalyse sowie Datensicherheit durch technische und organisatorische Maßnahmen sind zwingend zu berücksichtigen. Die zunehmende Verdatung unseres Alltagslebens führt dazu, dass umfassendste Datenprofile über uns alle entstehen, die Datensouveränität ist daher zu stärken und der Trend der allumfassenden Verdatung und Algorithmisierung muss mit Konzepten der Risikorelevanz und entsprechenden Schutz- und Nicht-Verarbeitungsvorgeben dieser Daten einhergehen.

Anders als es auf den ersten Blick erscheint, erweitert das Internet nicht nur meine Möglichkeiten, mich selbstbestimmt zu entwickeln. Teilweise ist das Gegenteil der Fall. Immer mehr Unternehmen nehmen für sich in Anspruch, vor mir zu wissen, was ich demnächst kaufen werde, wo ich meinen Urlaub verbringen möchte oder in wen ich mich verlieben könnte. Algorithmen filtern die unzähligen Angebote für mich heraus. Das ist vielleicht bequem, aber nicht unbedingt gut für unsere Gesellschaft. Intransparente Beeinflussung des Willensbildungsprozesses durch Hyper Targeting und Big Nudging müssen transparent werden. Dies gilt gerade auch für politische Kommunikation. Der Einsatz solcher Techniken, insbesondere in Wahlkampfzeiten, gehört reguliert, um für die notwendige Transparenz und Aufsicht zu sorgen.

Doch nicht nur die Nutzung und Ausnutzung von Daten über uns beeinflussen unser Handeln, unsere Kommunikation und soziales Zusammenleben. Wir erleben, wie im digitalen Diskurs eine Verrohung stattfinden, engagierte Menschen, ganz egal ob Feminist*innen, Politiker*innen, Ehrenamtliche, Journalist*innen oder Menschen mit Migrationshintergrund werden immer häufiger angefeindet, beleidigt und bedroht. Gerade von Mehrfachdiskriminierung betroffene Menschen erfahren zusätzlich Gewalt im Netz. Die Hoffnung, dass durch das Internet eine neue Debattenkultur und die Möglichkeiten des freien Wissenszugangs zu mehr Toleranz und Solidarität führen, wurde leider nicht erfüllt. Stattdessen entstehen derzeit abgeschottete Räume des selbstreferentiellen Meinungsaustausches. Hate Speech, Gewalt im Netz und Hasspropaganda stellen eine Bedrohung für unsere offene Gesellschaft dar. Einschüchterungen und Straftaten müssen mit allen rechtsstaatlichen Mitteln verfolgt werden, außerdem muss zivilgesellschaftliches Engagement im Kampf gegen Hate Speech gestärkt werden. Der Ausweitung der privaten Rechtsdurchsetzung widersprechen wir, stattdessen braucht es einen Ausbau der Kapazitäten und gezielte Schulungen bei Polizei und Staatsanwaltschaften in diesem Bereich. Zudem braucht es einfachere Wege solche Inhalte zu melden und anzuzeigen und eine Bundesregierung die es nicht länger verpasst, milliardenschwere Unternehmen an ihre gesellschaftliche und rechtliche Verpflichtung zu erinnern, entsprechende Inhalte konsequent zu überprüfen, zu löschen und an die Strafverfolgungsbehörden weiterzuleiten.
Aktuell beobachten wir, dass die Zahl rechtsextremer Straftaten zunimmt – erschütternde Beispiele sind Brandanschläge auf Flüchtlingsunterkünfte und gewaltsame Übergriffe mit fremdenfeindlichem Hintergrund. Und die Radikalisierung im Internet spielt dabei eine gewichtige Rolle. Mit allen rechtsstaatlichen Mitteln muss der Staat rechten Terror, alltäglichen Rassismus und institutionell verankerten Rassismus bekämpfen. Dazu zählt selbstverständlich auch das Strafrecht. Strafbarkeitslücken bei dem Verbreiten und Verwenden von Propagandamitteln und Kennzeichen verfassungswidriger Organisationen bei Handlungen im Ausland sind zu schließen und unter Strafe zu stellen. Zudem ist eine stärkere Berücksichtigung menschenverachtender Beweggründe bei der Strafzumessung gesetzlich zu verankern.