FRAKTIONSBESCHLUSS VOM 13.01.2017

» VERANTWORTUNG, FREIHEIT UND RECHT IM NETZ

Hass und Hetze drohen alltäglich zu werden. Hemmschwellen brechen weg. Vorurteile werden geschürt und Feindbilder bedient. Menschen werden beleidigt und bedroht. Hass und Hetze gegen Flüchtlinge und Muslime, Rassismus, Sexismus, Homophobie und Antisemitismus durchschwemmen Foren, soziale Netzwerke, Blogs und Kommentarspalten. Die Anschläge auf Flüchtlingseinrichtungen, Beleidigungen gegenüber MitarbeiterInnen in gemeinnützigen Vereinen oder von Kirchen und politisch Engagierten machen erneut deutlich: Hass und Hetze haben Konsequenzen im Handeln und führen auch zu mehr Gewalt. Das Netz befördert diese Dynamik und wirkt derzeit wie eine Art Brandbeschleuniger. Klick-Logiken kennen keine Menschenwürde. International hat sich 2016 gezeigt: Gesellschaftliche Meinungsbildung kann durch gezielte Falschinformationen, durch (auch geheimdienstliche) IT-Angriffe und Hacking, aber auch den Einsatz von „Social Bots" erfolgreich manipuliert werden.

Die Integrität von Kommunikation wird bewusst beeinflusst und zerstört, Falschinformationen über das Netz gezielt verbreitet. Zivilgesellschaftliche, journalistische und politische Akteurinnen und Akteure werden eingeschüchtert. All dies ist eine echte Gefahr für die Demokratie. Eine Gefahr, auf die Politik zielgenau und entschlossen reagieren muss.

Demokratinnen und Demokraten müssen die politische Auseinandersetzung gegen Hate und Fake führen. Es braucht klare Regeln, damit *alle* mehr Verantwortung im und für das Netz übernehmen, dem wichtigsten Kommunikationsraum unserer Zeit. Der intransparente Einsatz von Social Bots, das gezielte Verbreiten von Falschmeldungen und bewusste Manipulationen von Wahlen und politischen Entscheidungsprozessen übers Netz verlangen differenzierte, passgenaue Antworten. Genauso wie der Staat ländliche Regionen nicht aufgeben darf, darf er nicht zusehen, wie im Netz grundrechtsfreie Räume entstehen. Seiner Schutzverantwortung muss er gerecht werden. Die Zeit drängt.

Wir wollen einen **bundesweiten Aktionsplan „Verantwortung, Freiheit und Recht im Netz"** und legen hierfür Eckpunkte vor.

Rechtsstaatliche Antworten geben

Das Grundgesetz unterscheidet nicht zwischen analog und digital. Als grüne Bundestagsfraktion stehen wir für die Grundrechte der Meinungs-, Medien- und Informationsfreiheit. Meinungsfreiheit gilt auch für abseitige, oftmals schwer erträgliche Positionen. Gleichzeitig sind dem Verbreiten von Falschmeldungen, gerade, wenn die Rechte anderer, zum Beispiel ihre Persönlichkeitsrechte verletzt sind, Inhalte strafbar sind oder Tatsachenbehauptung erwiesen und bewusst falsch sind, durchaus schon heute enge rechtliche Grenzen gesetzt. Die rote Linie liegt also dort, wo rechtswidriges Handeln anfängt.

Die Grenzen sind in der digitalen wie der analogen Welt dieselben: Die Rechte anderer dürfen nicht verletzt und gegen die verfassungsmäßige Ordnung darf nicht verstoßen werden. Hier muss der Rechtsstaat klare Kante zeigen: Niemand darf allein gelassen werden, wenn er zum Beispiel für sein Engagement für die Gesellschaft beleidigt und bedroht wird. Niemand darf sich sicher dabei fühlen, wenn er andere menschenverachtend beschimpft, zur Gewalt aufruft oder sich volksverhetzend äußert. Auch gegen Falschmeldungen muss entschlossen vorgegangen werden.

Offensichtliche Verleumdungen und üble Nachrede müssen schnellstmöglich, allerspätestens jedoch nach 24 Stunden und entsprechender Prüfung durch die Unternehmen gelöscht werden. Zudem muss heute mehr denn je gelten: Strafverfolgungsbehörden müssen bestehendes Recht und bestehende Gesetze konsequent anwenden. Denn bei Rechtsverletzungen reichen bestehender Rechtsschutzmöglichkeiten (zum Beispiel Auskunfts-, Unterlassungs-, Beseitigungs- und Schadensersatzansprüche, Störer- und Verbreiterhaftung), die bestehenden Strafgesetze (zum Beispiel hinsichtlich Beleidigung, übler Nachrede, Verleumdung, Volksverhetzung, falscher Verdächtigung, Bedrohung, Nötigung, Aufforderung zu und Billigung von Straftaten) und die staatliche Pflicht zur Strafverfolgung grundsätzlich aus. Um sicherzustellen, dass sie durchgesetzt werden, müssen Polizei und Strafverfolgungsbehörden jedoch bestehende Instrumente konsequent anwenden. Zudem bedarf es vor allem entsprechender Schulungen und zusätzlicher MitarbeiterInnen. Die Kapazitäten bei Polizei und Justiz müssen darauf ausgerichtet sein, dass die mühselige Ermittlung der Täter nicht durch die personell bedingte Einstellung der Verfahren umgangen wird.

Der reflexhafte Ruf nach immer neuen Straftatbeständen führt nicht weiter. Auch angesichts der Massenhaftigkeit und der schnellen Verbreitung von Inhalten im Netz liegen das Problem und die rechtspolitische Aufgabe darin, bestehende individuelle Rechte und den staatlichen Strafanspruch wirksam durchzusetzen.

Sorgfaltspflichten für Dienstleister ausbauen und die Rechtsanwendung stärken

Die Bundesregierung toleriert bis heute, dass sich milliardenschwere Unternehmen mit teils monopolartigem Charakter nicht an geltendes deutsches und europäisches Recht halten. Sie missachten mit lapidaren Hinweisen auf die eigene Multinationalität, allgemeine Geschäftsbedingungen und sich selbst gegebene „Gemeinschaftsstandards" klare rechtliche Vorgaben. Das muss ein Ende haben. Selbstverpflichtungen reichen nicht. Die bisherigen Bemühungen der Bundesregierung reichen bei Weitem nicht aus. Mit medienwirksamen „Task Forces", offenen Briefen und immer neuen, folgenlosen Fristen hat Bundesjustizminister Maas bislang nichts Wesentliches zur Beseitigung der skizzierten Probleme beigetragen. Er ist weiter in der Pflicht. Digitale Gatekeeper müssen entschlossen in die Pflicht genommen werden, ihrer Verantwortung nachzukommen und geltendes Recht anzuwenden:

- Wird Recht offensichtlich verletzt, sind Unternehmen verpflichtet, Inhalte umgehend zu überprüfen und im gegebenen Fall rasch zu entfernen.
- Das gilt für strafbare Hate Speech genauso wie für erwiesene und bewusste Falschbehauptungen, die Persönlichkeitsrechte verletzen. Dieses „notice and takedown"-Verfahren ist bereits im deutschen Telemedienrecht als auch im EU-Recht (E-Commerce-Richtlinie) verankert. Gleichzeitig müssen in solchen Fällen Beweise gesichert werden, um gegebenenfalls Strafverfolgung zu ermöglichen und zivilrechtliche Ansprüche durchsetzen zu können.
- Die Unternehmen müssen verlässlich funktionierende Kommunikationswege und inländische Zustellungsbevollmächtigte für Beschwerden und Löschungswünsche von Betroffenen sicherstellen, ebenso für Anfragen von Ermittlungsbehörden. Heute scheitert oftmals sogar die Zustellung, weil zum Beispiel Facebook offiziell kein Büro in Deutschland hat. Gegebenenfalls bedarf es einer entsprechenden rechtlichen Verpflichtung, auf deren Notwendigkeit auch die Justizministerkonferenz bereits hingewiesen hat. Zudem brauchen wir neben bestehenden, weitere unabhängige Vermittlungsinstanzen und die Bereitschaft der Unternehmen, einen Ombudsmann/eine Ombudsfrau zu benennen und diese in die entsprechenden Gremien zu entsenden.

- Um auf etwaige Rechtsverstöße umgehend reagieren zu können, müssen die Unternehmen ausreichend und gut ausgebildetes Personal vorhalten, das Inhalte umgehend nach Kenntnisnahme entlang der deutschen und europäischen Rechtslage prüft. Dieses Personal, das sich täglich mit belastenden Inhalten beschäftigt, muss dabei von den Dienstleistern angemessen unterstützt werden. Wird ein Inhalt nach Prüfung durch den Dienstleister als strafbar und zu löschend eingeordnet, muss sichergestellt sein, dass es zu einer schnellen und konsequenten Weiterleitung an die Strafverfolgungsbehörden kommt. Diese müssen wiederum personell und fachlich in der Lage sein, gegen die UrheberInnen konsequent vorzugehen. Dazu gehört auch die Auskunftspflicht gegenüber den Strafermittlungsbehörden was die Identität von potenziellen RechtsverletzerInnen angeht.
- Es ist nicht akzeptabel, dass gegen diejenigen, die Hass und Hetze verbreiten, nur im absoluten Ausnahmefall ermittelt und sie zur Rechenschaft gezogen werden. Der Bund muss sich mehr engagieren, um Persönlichkeitsrechte und den staatlichen Strafanspruch wirksam durchzusetzen. Dazu gehört, Polizei und Justiz technisch und personell gemeinsam mit den Ländern dem digitalen Zeitalter angemessen auszustatten. Auch die internationale Zusammenarbeit bei der Strafverfolgung muss weiter verbessert werden.
- Es braucht gesetzliche Berichtspflichten: Die Unternehmen müssen regelmäßig transparent über ihre Bemühungen berichten und gegebenenfalls verpflichtet werden, entsprechende Evaluierungen vorzulegen. Das betrifft die Anzahl der erfolgten Meldungen, die Art ihrer Bearbeitung einschließlich des Zeitablaufs, die für die Erledigung eingesetzten Ressourcen und die Kriterien für die Erledigung.
- Es braucht zudem wirksame Sanktionen, wenn Dienstleister unmittelbar gegen die genannten Sorgfaltspflichten verstoßen oder ihre entsprechenden Organisations- und Aufsichtspflichten im Unternehmen verletzen. Dann müssen empfindliche Bußgelder verhängt werden, deren Höhe die wirtschaftliche Lage der Dienstleister erfassen und dabei insbesondere an die Umsätze anknüpfen muss. Auch an Gewinnabschöpfungen ist zu denken. Mit einem Antrag „Zukunftsfähige Unternehmensverantwortung – Wirksame Sanktionen bei Rechtsverstößen von Unternehmen“ (BT-Drs. 18/10038) haben wir bereits dargelegt, wie das geht.

Die bestehenden Rechtsschutzmöglichkeiten bleiben daneben unberührt. Im Rechtsstaat entscheiden die Gerichte über Rechtsstreitigkeiten. Das ist im Wege einstweiligen Rechtsschutzes auch sehr schnell und mit wirksamen Sanktionen möglich. Wir hoffen, dass es bald zu weiteren höchstrichterlichen Entscheidungen kommt, insbesondere hinsichtlich strafrechtlicher Dimensionen.

Die Zivilgesellschaft gegen Hass und Hetze stärken

Menschen, die sich tagtäglich gegen Hass und Hetze engagieren, die strafbare Inhalte melden und auf Konsequenzen hoffen, zählen auf die Unterstützung durch den Rechtsstaat und demokratische Politik. Die muss jetzt tatsächlich kommen! Wir werden nicht zulassen, dass das Vertrauen in demokratische und rechtsstaatliche Institutionen weiter erodiert. Ebenso wenig, dass die Menschen, die sich engagieren, resignieren oder gar vor Hass und Hetze im Netz kapitulieren.

Länder und Kommunen, alle relevanten gesellschaftlichen Kräfte, Medien, Vereine und Verbände, Gewerkschaften und Unternehmen, Wissenschaft, Kultur und Sport, Religions- und Weltanschauungsgemeinschaften sollten eingeladen werden, einen bundesweiten Aktionsplan „Verantwortung, Freiheit und Recht im Netz“ zu erarbeiten. Bestehende Kooperationen wie das nationale Komitee, das die No-Hate-Speech Kampagne des Europarats in Deutschland umsetzt, müssen verstetigt werden. Zivilgesellschaftliche Einrichtungen, die sich für Monitoring und Aufklärung

engagieren und die strafbaren Meinungsäußerungen im Netz, Radikalisierung und Verrohung der Debattenkultur entgegentreten, sollen stärker gefördert werden. Bußgelder und gegebenenfalls Gewinnabschöpfungen, die aufgrund von Pflichtverletzungen von Unternehmen verhängt werden, können hierfür verwendet werden. Wir wollen mehr Forschung, um strafbare Meinungsäußerungen sowie die Verletzung von Persönlichkeitsrechten im Netz zu bekämpfen. Dies ermöglicht zielgenauere Präventionsstrategien. Die Bundesregierung muss sich zudem auf EU- und internationaler Ebene dafür einsetzen, eine enge Zusammenarbeit und Vernetzung aller Akteure im Kampf gegen Hate Speech weiter zu stärken.

Falschmeldungen im Netz bekämpfen

In der freiheitlichen Demokratie gibt es keinen Anspruch – und schon gar nicht des Staates – auf absolute Wahrheit, und eine Zensur darf nicht stattfinden. Es ist aber notwendig, entschlossen gegen erwiesene oder bewusste Falschmeldungen vorzugehen, die von der Meinungsfreiheit verfassungsrechtlich nicht geschützt sind. Der Staat hat daher sicherzustellen, dass die bestehenden Ansprüche auf Widerruf, Unterlassung und Schadensersatz effektiv vor Gericht verfolgt werden können, und dass die staatlichen Strafverfolgungsbehörden strafrechtlich relevante falsche Behauptungen effektiv verfolgen können.

In der Zivilgesellschaft, den Medien und den politischen Institutionen muss eine Kultur von Wahrhaftigkeit und wechselseitigem Respekt gepflegt und gestärkt werden. Das beste Mittel gegen unlautere Verdrehung von Tatsachen, Verleumdung und Verrohung ist, wenn Demokratinnen und Demokraten gemeinsam für eine Kommunikation sorgen, die Respekt und Menschenwürde achtet, transparent, faktengestützt und auch selbstkritisch ist.

Um Freiheit zu wahren, bedarf es auch im Netz ständiger Achtsamkeit sowie des aktiven Engagements für demokratischen Diskurs und Respekt. Dies setzt zunächst eine möglichst hohe Medienkompetenz möglichst Aller voraus. In einer Zeit, in der alle möglichen Akteure problemlos publizieren und weiterverbreiten können, ohne dass sichergestellt ist, dass Publiziertes durchweg anerkannten journalistischen Sorgfaltspflichten entspricht, muss die Fähigkeit und die Bereitschaft gefördert werden, Inhalte kritisch zu hinterfragen und bewusst verfälschte und persönlichkeitsrechtsverletztende Nachrichten als solche zu erkennen. Daher bleibt im digitalen Zeitalter der Erwerb von Medienkompetenz – möglichst lebenslang – eine zentrale Herausforderung.

Abwegig ist allerdings, die Schaffung eines staatlichen „Wahrheitsministeriums“ auch nur zu erwägen. Das kann kein ernst gemeinter Vorschlag in einer pluralistischen Demokratie sein. Andere Vorschläge, wie zum Beispiel die Schaffung unabhängiger Einrichtungen zur Prüfung der Einhaltung grundlegender Sorgfaltspflichten, etwa in Anlehnung an das, was für Medienangehörige gilt, sollten dagegen diskutiert werden.

Die wenigen großen Plattformen, die heute einen erheblichen Teil dazu beitragen, dass Falschnachrichten – obwohl teilweise längst widerlegt – weiterverbreitet werden, müssen aktiv an der Verhinderung der Verbreitung von Falschmeldungen und Persönlichkeitsverletzungen mitwirken. Freilich dürfen ohnehin übermächtige Konzerne nicht in die Rolle von Zensoren gedrängt werden und noch stärker als bislang darüber entscheiden, was ein wünschenswerter Inhalt ist und was nicht. Auch wäre es datenschutzrechtlich höchst fragwürdig, wenn Unternehmen höchst aussagekräftige Datenbanken darüber anlegen müssten, wann wer welche politischen Artikel und Inhalte mit wem geteilt hat. Vor diesem Hintergrund werden wir die tatsächliche Sinn- und Durchsetzbarkeit einer Verpflichtung zur Gegendarstellung prüfen.

Den Einsatz von „Social Bots“ rechtlich regeln

Technik kann immer ambivalent eingesetzt werden – und wird dies auch häufig. Social Bots sind hierfür ein gutes Beispiel. Es gibt sinnvolle Anwendungen: Sie können dazu beitragen, sich tausendfach wiederholende Abläufe zu automatisieren und Menschen zu entlasten. Sie können dabei helfen, Wählerinnen und Wähler auf gesuchte Passagen in Wahlprogrammen hinzuweisen, Hilfesuchende auf Fundstellen für Rat und Tat aufmerksam zu machen oder Haterinnen und Hater automatisiert auf geltende Diskussionsregeln hinweisen.

Genauso können Social Bots aber dort, wo sie entsprechend programmiert und missbräuchlich eingesetzt werden, demokratische Diskurse vergiften. Sie täuschen vermeintliche Mehrheitsverhältnisse vor, die real nicht bestehen, und beeinflussen verdeckt demokratische Entscheidungsprozesse, ohne dass dies für die EmpfängerInnen der Bot-Botschaften erkennbar wäre. Den Einsatz von Social Bots per se zu verbieten, wie es in den vergangenen Wochen wiederholt gefordert wurde, würde allerdings der skizzierten Ambivalenz nicht gerecht werden. Klar ist aber: Selbstverpflichtungen allein reichen auch hier nicht aus. Zur effektiven Verhinderung der intransparenten Beeinflussung demokratischer Willensbildungsprozesse brauchen wir eine rechtlich implementierte Verpflichtung zur Offenlegung des Bot-Charakters von Botschaften. Wir sprechen uns für die gesetzliche Festlegung einer derartigen Transparenz- und einer Anzeigepflicht für den Einsatz von Social Bots aus.

Die IT-Sicherheit stärken

Berichte über große Hacking-Angriffe auf den Bundestag, Parteizentralen, das Bundeskanzleramt und Unternehmen machen deutlich, wie ernst die Lage ist. Dies hat auch der US-Wahlkampf gezeigt. Die Gefahr verheerender Hacks wächst täglich. Das von der Bundesregierung vorgelegte IT-Sicherheitsgesetz wird den aktuellen Herausforderungen zum Schutz privater Kommunikation und digitaler Infrastrukturen nicht ansatzweise gerecht. Das Nebeneinander von Strukturen, ein digitalpolitisches Wetteifern verschiedener Ministerien ohne Koordination, oftmals unklare Zuständigkeiten und fehlende rechtliche Vorgaben – all dies steht symptomatisch für die widersprüchliche IT-Sicherheitspolitik der Bundesregierung.

Die Bundesregierung tut so, als habe es die zahlreichen Erkenntnisse aus dem parlamentarischen Untersuchungsausschuss zum geheimdienstlichen Abhör- und Ausspähskandal nie gegeben. Rechtsstaatlich dringende Konsequenzen aus den Enthüllungen Edward Snowdens und der Aufklärung durch den Bundestag zieht man bis heute keine. Im Gegenteil: Überwachungsbefugnisse wurden massiv ausgebaut und die parlamentarische Kontrolle erschwert. Die Grundrechte auf Integrität und Vertraulichkeit informationstechnischer Systeme und auf informationelle Selbstbestimmung lässt die Bundesregierung nicht nur leer laufen, sie schwächt sie zusätzlich.

Ein ganzheitlicher Ansatz, um die IT-Sicherheit zu erhöhen, bleibt dringend nötig. Die Verantwortung darf nicht allein auf Nutzerinnen, Nutzer und Unternehmen abgewälzt werden. Dem Staat kommt eine – direkt aus unserer Verfassung abzuleitende – Schutzverantwortung zu: Sie gilt nicht nur für kritische Infrastrukturen (KRITIS), sondern für digitale Infrastrukturen und private Kommunikation insgesamt.

Die Themen IT-Sicherheit und Datenschutz sind im Innenministerium schlecht aufgehoben. Sie müssen endlich an allerhöchster Stelle mit klaren Verantwortlichkeiten bearbeitet werden. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) muss – zumindest in Teilen – unabhängig vom Bundesinnenministerium gestellt werden. Nur so kann es seinen Aufgaben tatsächlich gerecht werden. Um den stark gestiegenen Anforderungen zu begegnen, müssen die Ressourcen der Aufsichtsbehörden dringend weiter aufgestockt werden.

Es bedarf positiver und wettbewerbsrelevanter Anreize für die Wirtschaft, in gute IT-Sicherheitslösungen zu investieren. Durchgehende Ende-zu-Ende-Verschlüsselungen müssen bei allen IT-Großprojekten Standard werden. Ebenso muss freie und offene Software, die auch innovative Datenschutzkonzepte wie „Privacy by Design“ und „Security by Design“ berücksichtigt, sehr viel stärker gefördert werden. Sie sollte etwa in der öffentlichen Verwaltung verstärkt eingesetzt werden. Hier kommt dem Staat eine wichtige Vorbildfunktion zu. Dabei muss es nicht nur für Betreiber, sondern auch für die Hersteller von Hard- und Software Anreize zur Qualitätssicherung geben, beispielsweise durch Haftungsverpflichtungen oder Auditierungen.

Die bisherige IT-Sicherheitspolitik des Bundes erhöht die Sicherheit nicht, sie gefährdet sie. Denn sie hält unbeirrt an anlasslosen Massenspeicherungen oder dem anhaltenden staatlichen Aufkauf und die Verwendung von Sicherheitslücken und Zero Day Exploits fest, die gefährliche Lücken in Infrastrukturen reproduzieren und mitfinanzieren. Hier setzen wir uns weiterhin für ein klares gesetzliches Verbot ein. Insgesamt bedarf es einer echten Kehrtwende in der IT-Sicherheits- und Datenschutzpolitik und ein Sofortprogramm zur Erhöhung der IT-Sicherheit in Deutschland.