Freiheit versus Sicherheit

Europäische Diskussionen um die Regulierung des Internet

Künstliche Intelligenz kann helfen, diskriminierende und gefährliche Inhalte im Internet zu identifizieren. Doch die Automatisierung der Kontrolle löst nicht die grundlegenden Fragen der Plattform-Regulierung: Wie können Individuen am besten geschützt werden? Wie wird die öffentliche Sicherheit gewährleistet? Wie werden gleichzeitig Meinungs- und Informationsfreiheit gestärkt? Robert Gorwa zeichnet das Spannungsfeld am Beispiel der jüngsten Debatten in der EU um den Kinderschutz im Netz nach.

Robert Gorwa

2022 war ein außerordentlich arbeitsreiches Jahr für die Technologiepolitik in Europa. Die Europäische Kommission erarbeitete ein Gesetz zur Gewährleistung von Sicherheit und Grundrechtskonformität der Systeme Künstlicher Intelligenz; sie beschloss eine Richtlinie zur Verbesserung der Arbeitsbedingungen in der Plattformarbeit, sie legte ein Gesetz über digitale Dienste und ein Gesetz über digitale Märkte vor. Alle diese Regulierungsbemühungen zielten darauf ab, die Verbraucher besser zu schützen und die Verfahren und die Transparenz bei politisch wichtigen digitalen Infrastrukturen zu verbessern, von denen letztlich alle europäischen Bürger und Bürgerinnen abhängen.

Diese Maßnahmen werden weithin begrüßt, weil sie das Potenzial haben, eine die Individualrechte respektierende digitale Wirtschaft zu schaffen. Gleichzeitig ringen immer mehr Forschende und zivilgesellschaftliche Interessenvertretungen mit einer grundlegenden Spannung in der digitalen Politik der EU: Auf der einen Seite stehen die Freiheitsrechte der Bürger*innen, auf der anderen komplexe Sicherheitsanforderungen.

Ein gutes Beispiel dafür sind die Rechte von Kindern im Netz. Im vergangenen Frühjahr kündigte die Kommission eine Reihe neuer Vorschläge für Maßnahmen zum Online-Kinderschutz an. Dazu gehörten die Initiative „Neue europäische Strategie für ein besseres Internet für Kinder“ sowie der Entwurf für eine Verordnung mit „Vorschriften zur Verhütung und Bekämpfung des sexuellen Missbrauchs von Kindern“.

Dieser Entwurf, der das Europäische Parlament bereits durchlaufen hat, hat große Auswirkungen auf die digitale Welt. Regierungen und Inte-

ressengruppen üben seit über einem Jahrzehnt Druck auf Unternehmen aus, die Plattformen betreiben – vor allem soziale Netzwerke, aber auch Suchmaschinen und Anbieter von Cloud-Speichern –, damit sie technische Maßnahmen gegen die Verbreitung von als sozial schädlich eingestuften Inhalten ergreifen, beispielsweise von Bildern von Kindesmissbrauch und gewalttätiger extremistischer Propaganda. Bislang war dieser Druck jedoch weitgehend informell, und die Zusammenarbeit der Industrie verlief auf freiwilliger Basis.

So verwenden viele Plattformen kryptografische Hash Matching Tools wie zum Beispiel PhotoDNA von Microsoft. Diese Programme erstellen Fingerabdrücke von Nutzer-Uploads und gleichen sie mit Listen ab, die von Organisationen wie dem amerikanischen National Centre for Missing and Exploited Children gesammelt werden. Auf Druck von EU-Sicherheitsbeamten gründeten Facebook, Google, Twitter und Microsoft das Global Internet Forum to Counter Terrorism, dessen Datenbank mittlerweile von Unternehmen wie Amazon, Airbnb, Discord, Tumblr, Zoom, Mailchimp und Dropbox auf verschiedene Weise genutzt wird.

Der EU-Vorschlag zielt darauf ab, diese zwar freiwillige, aber doch erst durch staatlichen Druck und unter Androhung von Sanktionen zustande gekommene Zusammenarbeit durch

> „Unternehmen sollen jetzt dazu verpflichtet werden, Systeme zur automatischen Erkennung und Löschung von allen Inhalten einzusetzen, die den Missbrauch von Kindern begünstigen“

eine verbindliche Verordnung zu ersetzen. Unternehmen sollen jetzt dazu verpflichtet werden, Systeme zur automatischen Erkennung und Löschung von allen Inhalten einzusetzen, die den Missbrauch von Kindern begünstigen könnten – und in weit größerem Umfang als bisher.

Doch wie aussichtsreich ist dieses Vorhaben, wie wirksam wird die vorgeschlagene Verordnung Kinder vor Missbrauch schützen? Und welche Folgen hat das für andere Grundrechte – insbesondere das auf Freiheit? Tatsächlich sind die Unzulänglichkeiten bestehender Technologien zur automatisierten Inhaltsanalyse in vielen Studien bereits hinreichend belegt worden.

Robert Gorwa ist als Postdoktorand wissenschaftlicher Mitarbeiter der Forschungsgruppen Globalisierung, Arbeit und Produktion sowie Politik der Digitalisierung am WZB. Sein erstes Buch, über die Politik der Regulierung von Technologieunternehmen im globalen Kontext, wird bei Oxford University Press erscheinen.
robert.gorwa@wzb.eu

Erstens ist die automatisierte Inhaltsanalyse weder genau noch zuverlässig genug. Forschung zur Verarbeitung natürlicher Sprache hat vielfach gezeigt, dass sich potenziell problematische Inhalte von Onlinetexten und -gesprächen nur begrenzt finden lassen. Die automatisierte Analyse führt oft zu unfairen Ergebnissen und zur Benachteiligung von

> „Slang und umgangssprachliches Englisch werden von gängigen Systemen mit deutlich höherer Wahrscheinlichkeit als Hassrede gekennzeichnet oder entfernt“

Minderheitengruppen. Slang und umgangssprachliches Englisch, die in der Arbeiterklasse in den USA gesprochen werden, werden von

gängigen Systemen beispielsweise mit deutlich höherer Wahrscheinlichkeit als „Hassrede“ gekennzeichnet oder entfernt. Und die automatisierte Erkennung von Nacktheit oder sexuellen Aktivitäten in Fotos bringt oft falsch positive und falsch negative Ergebnisse.

Zweitens gibt es bei diesen Systemen schwerwiegende Transparenzprobleme, die dem Missbrauch Tür und Tor öffnen. Automatisierte Systeme zur Moderation von Inhalten verfügen zumeist nur über begrenzte Sicherheitsvorkehrungen. Die Datenbanken werden nicht überprüft und könnten auf viele Arten genutzt werden, die über das eigentliche Ziel der öffentlichen und individuellen Sicherheit hinausgehen. Wie The Times kürzlich berichtete, hat die britische Regierung beispielsweise versucht, Fingerabdrücke von Videos zu erstellen, die Flüchtlinge beim Überqueren des Ärmelkanals in einem positiven Licht zeigen. Die neuen Technologien wurden also missbraucht, um Imagepflege in einem aktuellen Skandal zu betreiben. Sehen wir einer Zukunft entgegen, in der Bürger und Bürgerinnen der Polizei oder EUROPOL gemeldet werden, weil ihr Telefon eines ihrer Fotos fälschlicherweise als illegal eingestuft hat? Könnten die neuen Systeme dazu genutzt werden, Druck auf Kritiker, Journalistinnen, auf die Zivilgesellschaft auszuüben?

> „Werden wir zukünftig der Polizei oder EUROPOL gemeldet, weil unser Telefon ein Foto fälschlicherweise als illegal eingestuft hat?“

Drittens: Stellen wir uns (gegen alle Wahrscheinlichkeit) vor, die groß angelegten automatischen Moderationssysteme würden perfekt funktionieren – das heißt ohne Overblocking (also das übermäßige Sperren von Inhalten) oder systematische Verzerrungen. Selbst dann würden sie immer noch große politische Probleme mit sich bringen, die in den Debatten um ihren breiteren Einsatz nicht ausreichend diskutiert werden. Schon jetzt treiben diese Technologien die Undurchsichtigkeit und die Komplexität der techno-sozialen bürokratischen Infrastrukturen voran, die die digital vermittelte Meinungsäußerung steuern. Je tiefer wir diese Systeme in unsere Geräte eindringen lassen, desto brisanter werden diese Probleme.

In der Debatte um die Verbreitung urheberrechtlich geschützter Inhalte im Internet werden die europäische Urheberrechtsrichtlinie und die Verpflichtung zum Einsatz technischer Upload-Filter zur Überprüfung von Inhalten kontrovers diskutiert. Gleichzeitig plädieren Kinderschutzgruppen und Sicherheitsbehörden für eine intensivere Überprüfung und den Abgleich potenziell illegaler Inhalte auch mit Methoden, die die Endverschlüsselung umgehen könnten, indem sie direkt auf den Telefonen und Computern der Menschen eingesetzt werden.

Sicherheitsexperten und Kryptografinnen haben bereits ihre Einwände gegenüber dieser Art von Entwicklung geäußert; sie reichen von der Verletzung der Grundsätze der Sicherheitstechnik bis hin zu Warnungen vor feindlichen Angriffen. Datenschutzexperten, darunter der Europäische Datenschutzausschuss und der Europäische Datenschutzbeauftragte, veröffentlichten im Sommer 2022 ihre Einschätzung, dass die von der Kommission vorgeschlagenen Maßnahmen zur digitalen Sicherheit ernsthafte Risiken für die Grundrechte darstellten. Dennoch setzt die Verordnung ihren langsamen Marsch durch das Europäische Parlament und den Rat fort.

Die Bemühungen der EU, die Freiheitsrechte der Verbraucher durch eine vorsichtige Regulierung der Plattformen zu schützen, stehen in offensichtlichem Widerspruch dazu, dass eben diese Rechte im Namen der öffentlichen Sicherheit und des Kinderschutzes untergraben werden. Wie kommt es zu diesem Paradox? Einige amerikanische Politikbeobachter sind überzeugt, dass die EU schlicht inkompetent sei. Ihre Regulierungsbehörden könnten nicht mit dem technologischen Fortschritt mithalten,

> „Bleibt Europa das kleine Kind auf dem Rücksitz, das keine Ahnung hat, wohin die Reise geht?“

und durch das Fehlen europäischer Technologieunternehmen sei Europa dazu verdammt, für immer das kleine Kind auf dem Rücksitz zu bleiben, das keine Ahnung hat, wo die Reise hingeht.

Die Realität ist natürlich weitaus komplizierter. Sie lässt sich erstens teilweise durch die komplizierte mehrstufige politische Entscheidungsstruktur der EU erklären. Die mehr als zwanzig Generaldirektionen der Europäischen Kommission haben enorm unterschiedliche Kompetenzen und Steuerungsstrategien in Bezug auf digitalpolitische Fragen. Die Generaldirektion Connect verfügt über sehr fähige politische Entscheidungsträger, und die von ihnen erstellten Entwürfe, wie beispielsweise der jüngste Rechtsakt über digitale Dienste, sind in der Regel zurückhaltend, evidenzbasiert und enthalten selten pauschale, technologisch nicht umsetzbare Forderungen. Die Generaldirektion Inneres hingegen ist viel stärker auf die Innenminister und Sicherheitsinteressen in den Hauptstädten der Mitgliedsstaaten ausgerichtet.

> „Die mehr als zwanzig Generaldirektionen der Europäischen Kommission haben enorm unterschiedliche Kompetenzen“

Diese institutionelle Zusammensetzung bedeutet auch, dass bestimmte Einheiten der Kommission anfällig sind für Versuche von Lobbyisten, Einfluss auf die Gesetzgebung zu nehmen. Wenn eine Lobbygruppe die Einheiten der Kommission, die sich mit digitaler Politik befassen, nicht überzeugen kann, kann sie anderswo ein offeneres Ohr finden – etwa bei Kommissaren, die engere Verbindungen zur Strafverfolgung und zum Sicherheitsapparat haben.

Außerdem geht es ja nicht um eine rein europäische Debatte. Einige der zentralen Akteure, die beim Entwurf der EU-Verordnung zur Bekämpfung des sexuellen Missbrauchs von Kindern mitdiskutierten, stammen nicht aus Europa, sondern sind in den USA ansässig. So war laut der Website netzpolitik.org ein Unternehmen des zum Risikokapitalgeber gewordenen Hollywood-Stars Ashton Kutcher und seiner ehemaligen Partnerin Demi Moore eine zentrale Kraft bei der Lobbyarbeit für die EU-Gesetzgebung. Politische Lobbygruppen wissen genau, dass die EU-Kommission globalen Einfluss hat. Sie versuchen, auf diesem Weg Regulierungen voranzubringen, die in den USA oder anderen Staaten keine Chance hätten.

Ob die Strategie der Lobbygruppen tatsächlich wirksam ist, wird wesentlich davon abhängen, wie die EU-Mitgliedsstaaten reagieren. In Deutschland gab es eine lebhafte Diskussion über die EU-Vorschläge, die in einen offenen Konflikt zwischen der SPD auf der einen und den Grünen und der FPD auf der anderen Seite führte (dass diese sich gegen die EU-Politik und ihre Bemühungen um eine verpflichtende Inhaltskontrolle stellt, wird kaum überraschen). Auch im Jahr 2023 werden Digitalexpert*innen höchst aufmerksam verfolgen, wie es in Berlin weitergeht.

Literatur

Abelson, Hal/Anderson, Ross/Bellovin, Steven M. et al.: Bugs in Our Pockets: The Risks of Client-Side Scanning. 2021. arXiv. DOI: 10.48550/arXiv.2110.07450.

Gesellschaft für Freiheitsrechte: Chatkontrolle: Mit Grundrechten unvereinbar. 2022. Online: https://freiheitsrechte.org/themen/freiheit-im-digitalen/chatkontrolle (Stand 21.02.2023).

Gorwa, Robert/Binns, Reuben/Katzenbach, Christian: „Algorithmic Content Moderation: Technical and Political Challenges in the Automation of Platform Governance“. In: Big Data & Society, 2020, Jg. 7, H. 1. DOI: 10.1177/2053951719897945.