



Sofortprogramm für ein sicheres Internet

Forderungen an die Bundesregierung zur Wahlperiode des 21. Deutschen Bundestags

Einleitung

Die vergangene Legislaturperiode hat gezeigt, dass Fortschritte beim Schutz vor digitaler Gewalt und für ein sicheres Internet möglich sind. Mit der Reform des Formerfordernisses für Strafanträge im Rahmen des Gesetzes zur weiteren Digitalisierung der Justiz, der Verabschiedung des Digitale-Dienste-Gesetzes (DDG) und der offiziellen Aufnahme der Arbeit des deutschen Digital Services Coordinators (DSC) wurden wichtige Schritte unternommen. Diese Maßnahmen erleichtern es Nutzer*innen, gegen rechtswidrige Inhalte auf Plattformen vorzugehen, und stärken die behördliche Aufsicht über digitale Dienste.

Dennoch bleiben gravierende Versäumnisse bestehen. Wichtige im Koalitionsvertrag angekündigte Reformen wurden nicht umgesetzt. Ein zentrales Gesetz gegen digitale Gewalt, das Betroffenen einen einfacheren Zugang zur privaten Rechtsdurchsetzung ermöglicht, fehlt weiterhin. Auch eine dringend benötigte Reform des Melderechts wurde nicht mehr verabschiedet, obwohl bereits Entwürfe und Stellungnahmen vorliegen. Diese Lücken schwächen den Schutz von Nutzern und den Zugang zum Recht und führen damit zu einer Gefährdung unseres demokratischen Diskurses.

Die neue Bundesregierung steht vor der Herausforderung, die Rechtsdurchsetzung im digitalen Raum nachhaltig zu verbessern. Plattformen müssen konsequenter in die Pflicht genommen und bestehende Regelungen zur Plattformhaftung weiterentwickelt werden. Gleichzeitig gilt es, bestehende Lücken im Strafrecht zu schließen, um Betroffene wirksam zu schützen. Die letzten Jahre haben gezeigt, dass es politisch möglich ist, Maßnahmen für ein sicheres Internet auf den Weg zu bringen – nun gilt es, die verbleibenden Lücken konsequent anzugehen.

Die Plattformregulierung in der EU zum Schutz vor Desinformation und digitaler Gewalt steht zunehmend unter Druck. Teilweise stellen US-Tech-Unternehmen die Einhaltung europäischer Digitalgesetzgebung sogar grundsätzlich in Frage. Einige Beispiele: Die Diskreditierung der EU-Regulierung als Zensur durch Elon Musk, das Einschränken der Faktenchecks durch Mark Zuckerberg oder das Zurückfahren von Moderation. Gerade jetzt braucht es daher entschlossene Regulierung und wirksame Schutzmaßnahmen. Die Gefahr: Nutzende werden von Desinformation und gewaltvollen Inhalten auf den Social Media Plattformen überflutet. Das gefährdet nicht nur Einzelne, sondern auch unsere Demokratie.

Dieses Papier skizziert konkrete Schritte, die kurzfristig ergriffen werden können, um den Schutz vor digitaler Gewalt effektiv zu stärken und ein sicheres Internet für alle Nutzenden zu schaffen:

1. **Durchsetzung des Digital Services Act (DSA) auf nationaler Ebene und Einsetzen für die Weiterentwicklung auf europäischer Ebene**
2. **Reform der absoluten Antragsdelikte bei Verbreitung von Inhalten**
3. **Reform der Privatklagedelikte bei Verbreitung von Inhalten**
4. **Ein Gesetz gegen digitale Gewalt und die Reform des Auskunftsanspruchs nach TDDDG**
5. **Einführung eines Tatbestandes zur Regelung der Strafbarkeit der Herstellung von nicht einvernehmlichen sexualisierten Deepfakes**
6. **Verpflichtender Hinweis auf den Ausgang des Strafverfahrens**
7. **Zugang zu den Gerichten: digitale Verfahren zum Schutz der Persönlichkeitsrechte**
8. **Einsetzen auf europäischer Ebene zur Reform über die Regelung der gerichtlichen Zuständigkeiten**
9. **Reform des Melderechts**
10. **Finanzielle Absicherung von Anlaufstellen für Betroffene**

1. Plattformregulierung: Durchsetzung des Digital Services Act auf nationaler Ebene und Einsetzen für die Weiterentwicklung des DSA

Das Problem: Der Digital Services Act (DSA), das europäische "Internetgrundgesetz", ist seit dem 17. Februar 2024 vollständig anwendbar. Online-Plattformen und Suchmaschinen sind seither nach dem EU-Digitalgesetz verpflichtet, Risiken für die Gesellschaft (u.a. für Wahlen, Kinder- und Jugendschutz oder die Würde des Menschen) unter anderem durch die Anpassung ihrer Algorithmen sowie durch die Moderation von Inhalten zu minimieren.

Die Plattformen sind in der Pflicht, die Risiken, die von ihnen und ihrer Funktionsweise ausgehen, einzuschätzen und darzulegen, wie sie diesen Risiken begegnen wollen. Sie müssen außerdem Forschenden Zugang zu Daten gewähren, damit diese systemischen Risiken erforschen können.

Weiterhin haben alle Nutzenden seit Einführung des DSA das Recht, rechtswidrige Inhalte mithilfe plattforminterner Meldewege zu melden und interne Beschwerde bei der Plattform einzulegen, sollte die Plattform den Inhalt nicht entfernen.

Die im DSA vorgegebenen Maßnahmen können aber nur Wirkung erzielen, wenn der DSA auch konsequent durchgesetzt wird. Dabei spielt die Aufsicht durch die Europäische Kommission und die nationalen Aufsichtsbehörden, in Deutschland durch die Bundesnetzagentur, eine entscheidende Rolle. Hier besteht dringend Handlungsbedarf, denn bisher ist zu konstatieren, dass die Plattformen den DSA nicht konsequent umsetzen:

- **Meldewege:** Viele der großen Plattformen haben Meldewege aufgesetzt, die alles andere als benutzerfreundlich sind, obwohl das explizit vom DSA vorgeschrieben wird.
- **Risikoberichte:** Auch die ersten von den Plattformen veröffentlichten Risikoberichte lassen wichtige Fragen offen und stellen die für die Öffentlichkeit dringend notwendige Transparenz nicht her.
- **Datenzugang für Forschende:** Kaum eine Plattform gewährleistet einen nutzbringenden Zugang zu Daten.

Die Europäische Kommission hat bereits Verfahren gegen viele der sogenannten VLOPS (Very Large Online Platforms) wegen Verstoßes gegen den DSA eingeleitet. Doch auch den nationalen DSCs kommt eine wichtige Bedeutung zu: Sie sollen u.a. außergerichtliche Streitbelegungsstellen und vertrauenswürdige Hinweisgeber zulassen, denen eine wichtige Rolle bei der DSA-Aufsicht zukommt. In Deutschland gibt es hiervon erst jeweils eine Stelle. Im Board der DSCs sollte Deutschland sich zudem in die gesamteuropäische Plattformaufsicht u.a. zum Thema Minderjährigenschutz und personalisierte Werbung aktiv einbringen. Hierfür braucht es jedoch ausreichend Ressourcen, die bisher nicht vorhanden sind.

Die Maßnahme: Bereitstellung ausreichender finanzieller und personeller Ressourcen für die Bundesnetzagentur (BNetzA) zur Kontrolle und Durchsetzung der im DSA vorgeschriebenen Pflichten; Nutzen der Möglichkeiten auf europäischer Ebene, sich für eine Weiterentwicklung des DSA einzusetzen.

2. Strafrecht: Reform der absoluten Antragsdelikte §§ 185 ff. StGB und § 33 KUG

Das Problem: Ermittlungsverfahren wegen Beleidigungsdelikten und Bildrechtsverletzungen im Internet werden von Staatsanwaltschaften überwiegend eingestellt. Dabei wird von den Strafverfolgungsbehörden regelmäßig verkannt, dass die Wirkung von Beleidigungen und übler Nachrede im Internet weit über den einzelnen Betroffenen hinausgeht. Es kann jedoch nicht Privatsache der Betroffenen sein, wenn sie von anonymen Tätern und Täterinnen in aller Öffentlichkeit bloßgestellt, beleidigt und diffamiert werden. Die veränderten Umstände des Internets mit der als schwerwiegender eingestuften Nutzung des geschriebenen Wortes und der hohen Reichweite und Verbreitung solcher Delikte, hatte schon das Bundesverfassungsgericht angemerkt. Derzeit hängt die Strafverfolgung zu häufig davon ab, ob die Betroffenen von den rechtswidrigen Inhalten überhaupt Kenntnis erlangen. Zusätzlich müssen Betroffene sowohl die Zeit, als auch die Kraft mitbringen zur Stellung der notwendigen Strafanträge.

Die Maßnahme: Absolute Antragsdelikte, vor allem Äußerungsdelikte und Bildrechtsverletzungen, sollten künftig als **relative Antragsdelikte** ausgestaltet werden, wenn sie durch das Verbreiten von Inhalten begangen werden. Dies würde es der Strafverfolgung ermöglichen, in geeigneten Fällen das öffentliche Interesse zu bejahen und Ermittlungen auch ohne Antrag aufzunehmen. Das könnte bspw. bei

öffentlichkeitswirksamen und aus menschenfeindlichen Motiven hervorgehenden Anfeindungen von ehrenamtlich engagierten Personen, wie kommunalpolitisch Engagierten Parteimitgliedern, Mitgliedern der örtlichen freiwilligen Feuerwehr oder Aktiven im Heimatverein, geschehen. Dabei erfüllt das Strafrecht nicht nur eine strafende Wirkung gegenüber der Tatperson, sondern ebenfalls eine Abschreckung und damit Prävention eines immer gewaltvolleren Tones im digitalen Raum.

3. Strafrecht: Reform der Privatklagedelikte § 373 StPO

Das Problem: Die Strafverfolgung scheidet oftmals an einer Verfahrenseinstellung unter Verweis auf den Privatklageweg gemäß § 374 StPO. Dies geschieht selbst dann, wenn ein Verfolgungsinteresse seitens der Betroffenen besteht und ein Strafantrag gestellt wird. Der Verweis auf den Privatklageweg ist auch dann ohne weiteres durch Beschluss möglich und für die Betroffenen nicht anfechtbar - weder auf dem Weg der Beschwerde noch ist ein Klageerzwingungsverfahren statthaft. Von dieser Möglichkeit der Einstellung wird vielfach (mutmaßlich auch zur Entlastung der Justiz) Gebrauch gemacht, auch wenn es sich nach Nr. 86 Abs. 2 RiStBV wegen menschenverachtenden Beweggründen verbieten sollte.

Die Maßnahme: Es empfiehlt sich daher dringend die Delikte der §§ 185 ff. StGB und § 33 KUG nicht nur als relative Antragsdelikte auszugestalten, sondern zusätzlich auch aus dem Katalog der Privatklagedelikte auszunehmen, wenn diese durch Verbreiten von Inhalten begangen werden. Allerdings ist es ebenfalls unbedingt erforderlich, dass Strafverfolgungsbehörden und die Justiz mit den notwendigen Ressourcen ausgestattet werden. Damit können Tatpersonen konsequent verfolgt und das Vertrauen in unseren Rechtsstaat gestärkt werden.

4. Strafprozessrecht: Verpflichtender Hinweis auf den Ausgang eines Verfahrens, 406d StPO

Das Problem: Betroffene digitaler Gewalt werden aktuell nur auf Antrag (§ 406d StPO) über den Ausgang eines gerichtlichen Strafverfahrens informiert.

Nach der Anzeige erhalten sie zwar Informationen über die Einstellung des Verfahrens, jedoch oft keine oder unzureichende Auskünfte über dessen weiteren Verlauf oder Abschluss. Das schafft eine erhebliche Informationsungleichheit, die negative Folgen hat: Viele Betroffene haben den Eindruck, dass Strafverfahren nach der Anzeige häufig eingestellt oder nicht konsequent weiterverfolgt werden. Das Strafrecht kann so seine volle generalpräventive Wirkung nicht entfalten.

Die Maßnahme: Es braucht mindestens einen verpflichtenden Hinweis auf die Möglichkeit der Antragstellung nach § 406d StPO. Darüber hinaus sollten Betroffene von digitaler Gewalt auch ohne Antragstellung über den Ausgang des Verfahrens informiert werden.

5. Strafrecht: Schließung der Strafbarkeitslücke für die Herstellung von nicht-einvernehmlichen sexualisierten Deepfakes

Das Problem: Mit ein paar Klicks lassen sich KI-generiert täuschend echt wirkende Missbrauchsbilder- und Videos erstellen – ganz einfach auf Internetseiten oder mit sogenannten Nudification Apps, die in den Appstores frei zugänglich sind. Dabei wird oft ein Foto aus dem Whatsapp-Status oder vom LinkedIn Profil der betroffenen Person kopiert und per App in einen sexualisierten Kontext gesetzt. Davon sind längst nicht mehr ausschließlich Personen des öffentlichen Lebens wie Giorgia Meloni oder Taylor Swift betroffen, sondern zunehmend auch Privatpersonen. Betroffen sind vor allem Frauen und Mädchen.

Diese Fälle des Missbrauchs sind bisher nur rudimentär im Gesetz abgebildet. § 201a StGB greift nur in seltenen Fällen und § 33 KunstURG fungiert als Auffangtatbestand. Verfolgt wird auf dieser Grundlage viel zu selten und zugleich wird das gravierende Unrecht des sexuellen Missbrauchs als Eingriff in das Recht auf sexuelle Selbstbestimmung nicht abgebildet. Beide Delikte sind sowohl Antrags- als auch Privatklagedelikte.

Die Maßnahme: Die Verbreitung von nicht einvernehmlich erstellten sexualisierten Deepfakes darf nicht länger als Bagatelldelikt behandelt werden. In der folgenden Legislaturperiode sollte ein eigener Straftatbestand dafür geschaffen werden, der auch die bloße Herstellung von nicht einvernehmlich erstellten sexualisierten Deepfakes erfasst. Denn diese werden oftmals auf mobilen Datenträgern oder gar in Cloud-diensten online gespeichert und können jederzeit in den Umlauf gelangen. Die Folgen für Betroffene sind zu gravierend.

6. Zivilrecht: Ein Gesetz gegen digitale Gewalt

Das Problem: Das zivilrechtliche Vorgehen gegen digitale Gewalt ist derzeit vor allem langwierig, kostenintensiv und in vielen Fällen nicht durchführbar, da es gerade häufig an der Identifizierung der Tatperson im digitalen Raum scheitert. Bestehende zivilrechtliche Möglichkeiten, die Anonymität bei Rechtsverletzungen zu durchbrechen, erweisen sich als nicht wirksam und zugleich kostenintensiv und kommen daher kaum je zur Anwendung. In der letzten Legislaturperiode wurden deshalb zunächst durch das Bundesjustizministerium Eckpunkte für ein Gesetz gegen digitale Gewalt vorgestellt, sowie ein Diskussionsentwurf durch das BMJ für ein Gesetz zur Stärkung der privaten Rechtsdurchsetzung im Internet veröffentlicht, zu welchem außerdem bereits Stellungnahmen von Verbänden und Organisationen eingeholt wurden.

Die Maßnahme: Das Gesetz sollte nun durch die nächste Bundesregierung zügig auf den Weg gebracht werden. Es muss Betroffenen in der Zukunft ein funktionierendes Verfahren an die Hand geben, die Identität der Täter*innen zu ermitteln, um gerichtlich gegen sie vorgehen zu können. Der Gesetzgeber sollte in der nächsten Legislaturperiode dafür sorgen, dass Betroffene mit nur einem einzigen Verfahren – sowohl bei sozialen Netzwerken als auch bei Internetzugangsdiensten – an die notwendigen Daten gelangen können. Hierfür kann an den bereits vorliegenden Diskussionsentwurf angeknüpft werden und somit Betroffenen von digitaler Gewalt zeitnah die private Rechtsdurchsetzung erheblich erleichtert werden.

7. Zugang zum Recht: Zugang zu den Gerichten und digitale Verfahren

Das Problem: Im digitalen Zeitalter sind Persönlichkeitsrechtsverletzungen durch soziale Netzwerke allgegenwärtig – sie betreffen nicht nur Personen des öffentlichen Lebens, sondern auch normale Bürgerinnen und Bürger, Journalisten und Journalistinnen und andere gesellschaftliche Akteure. Während presserechtliche Streitigkeiten mit klaren wirtschaftlichen Anreizen für die Beteiligten seit Jahrzehnten vor Gericht ausgetragen werden, bleibt der Zugang zum Recht für Betroffene in sozialen Netzwerken stark eingeschränkt.

Betroffene sehen sich trotz bestehender rechtlicher Ansprüche oft außerstande, Plattformbetreibende in die Verantwortung bei der Entfernung der Inhalte zu nehmen, da das ungleiche Machtverhältnis abschreckend wirkt. Zudem bestehen erhebliche finanzielle Hürden: Die potenziellen Kosten eines Verfahrens belaufen sich schnell auf mehrere tausend Euro. Auch die langen Verfahrensdauern – oft Monate oder Jahre – verhindern effektiven Rechtsschutz.

Diese strukturellen Defizite führen dazu, dass Persönlichkeitsrechtsverletzungen im digitalen Raum häufig folgenlos bleiben, während Betroffene mit erheblichen persönlichen und finanziellen Belastungen konfrontiert sind. Es besteht dringender Handlungsbedarf, um den Zugang zum Recht zu verbessern und effektive Mechanismen gegen digitale Persönlichkeitsrechtsverletzungen zu etablieren.

Die Maßnahme: Bereits die vorherige Bundesregierung hatte sich die Einführung bürgerfreundlicher digitaler Verfahren zur gerichtlichen Durchsetzung von Kleinforderungen zum Ziel gesetzt. Nach unserem Dafürhalten sollten digitale Verfahren gerade auch Persönlichkeitsrechtsverletzungen in elektronischen Informations- und Kommunikationsdiensten (Wortlaut: TMG; DSA: Vermittlungsdienste) umfassen. Dies würde den Zugang zum Recht erheblich verbessern.

8. Zugang zum Recht: Reform gerichtlicher Zuständigkeiten

Das Problem: Ein Beispiel: Ein Politiker nutzt ihren Facebook-Account für ihre politische Arbeit. Facebook sperrt den Account und die Politikerin möchte gerichtlich gegen die Sperrung vorgehen. Nach derzeitiger sich verstetigender Gerichtspraxis und Anwendung europäischen Rechts (EuGVVO) würde er wahrscheinlich an irische Gerichte verwiesen werden. Das gleiche gilt für einen Journalisten, eine Aktivistin auf X oder einen Abteilungsleiter auf LinkedIn. Die Kosten eines Verfahrens in Irland sind jedoch um ein Vielfaches höher als in Deutschland. Es müsste eine irische Anwaltskanzlei gefunden und mandatiert werden. Kosten für die Übersetzung fallen an. Zusätzlich handelt es sich in Irland um eine vollkommen fremde Rechtsordnung.

Faktisch bedeutet dies für den Politiker, dass er nicht mehr auf Facebook aktiv sein und Personen dort erreichen kann. Für Nutzende von Berufsplattformen wie LinkedIn würde das bedeuten, dass für sie ein Rechtsschutz in Deutschland wahrscheinlich ausgeschlossen ist.



Hintergrund ist der europäische Verbraucherbegriff. Wer Online-Plattformen nutzt, verwendet diese unter Umständen zu verschiedenen Zwecken. Nach der derzeitigen Gerichtspraxis kann niemand mehr Verbraucher sein, der jemals seine berufliche Tätigkeit in sozialen Medien thematisiert, sei es als Hinweis im Social Media Profil oder durch öffentlich getätigte Äußerungen.

All diese Menschen könnten soziale Netzwerke nur noch in Irland verklagen, um z.B. ihre Profile entsperren zu lassen, oder auf Unterlassung gegen die Online-Plattformen zu klagen, sollten diese rechtswidrige Inhalte auch nach Meldung nicht entfernen. Das traut sich so gut wie niemand zu und gibt den Plattformen dadurch freie Hand.

Die Maßnahme: Es ist zwingend erforderlich, dass Nutzende ihre Rechte unter zumutbaren Bedingungen durchsetzen können. Es sollte Gerichten nicht möglich sein, Verfahren gegen Plattformen dauerhaft einfach ins Ausland zu verweisen, wo weder die Erfolgsaussichten noch die Kosten für Betroffene berechenbar sind. Die gerichtliche Durchsetzung der Rechte von Nutzenden sollte am Wohnort möglich sein. In der DSGVO ist dies durch eine Zuständigkeitsregelung explizit erfasst (Art. 79 DSGVO), im DSA hingegen nicht. Wir empfehlen daher die **Schaffung eines Gerichtsstands für Nutzende von Online-Diensten am Wohnsitz**, entweder durch Anpassung der EuGVVO oder durch Einführung eines solchen Gerichtsstandes im Rahmen des DSA.

9. Öffentliches Recht: Reform des Melderechts

Das Problem: Betroffene digitaler Gewalt befürchten stets, dass persönliche Informationen über sie herausgefunden und im Rahmen digitaler Angriffe öffentlich gegen sie verwendet werden können. Diese Angst ist berechtigt, denn es ist eine beliebte Strategie, Informationen wie die Privatanschrift, den Namen der Schule der Kinder oder die Adressen von Familienangehörigen auszukundschaften und gezielt einzusetzen, um Menschen einzuschüchtern.

Der Schutz der Privatanschrift hat dabei oberste Priorität. Denn eine einfache Melderegisterauskunft gemäß § 44 Abs. 1 BMG ermöglicht ohne Begründung den Zugriff auf die Wohnanschrift – oft auch auf den Wohnort von Partner*innen und Kindern der Betroffenen. Auf diese Weise wird aus digitaler Gewalt schnell ein analoges Bedrohungsszenario. Dieses beeinträchtigt Betroffene massiv in ihrer Sicherheit.

In der vergangenen Legislatur wurde intensiv an einem Dritten Gesetz zur Änderung des Bundesmeldegesetzes gearbeitet (3. BMGÄndG). Hierbei wurde auch bereits eine Sachverständigenanhörung im Innenausschuss des Bundestages durchgeführt, bei der wichtige Impulse zur Gesetzesinitiative vorgetragen wurden. Das Gesetz wurde allerdings nicht mehr verabschiedet und es besteht insbesondere für Betroffene von digitaler Gewalt weiterhin ein unzureichender Schutz ihrer privaten Adressdaten.

Die Maßnahme: Es braucht jetzt schnell aufbauend auf der Vorarbeit die Einarbeitung von Änderungsvorschlägen und schließlich die Verabschiedung eines Gesetzes zur Reform des Melderechts. Hierbei sollte insbesondere bei der **Melderegisterauskunft** (§44 BMG) und der **Melderegistersperre** (§51 BMG) nachgebessert werden. Insbesondere sollten die Voraussetzungen für die Erteilung einer Melderegisterauskunft verschärft werden, indem zum Beispiel zur Abfrage an eine Glaubhaftmachung eines berechtigten Interesses

geknüpft wird, und Betroffene über eine Abfrage auch in Kenntnis gesetzt werden. Außerdem braucht es eine zeitliche Ausweitung der Geltungsdauer von erteilten Melderegistersperren.

10. Schutz Betroffener: Finanzielle Absicherung von Anlaufstellen/ Einrichtung einer zentralen Plattform für Hilfestellungen

Das Problem: Betroffene von digitaler Gewalt werden auch heute noch viel zu oft allein gelassen. HateAid ist nach wie vor die einzige bundesweit tätige Stelle für psychosoziale Beratung ausschließlich für Betroffene digitaler Gewalt. Bisherige Förderungen sind in der Regel eng befristet und über eine Verlängerung wird meist kurzfristig entschieden, was den Organisationen und ihren Mitarbeitenden kaum Planungssicherheit bietet und gerade in Zeiten des Fachkräftemangels zu erheblichen Schwierigkeiten führt, besonders ausgebildetes und geschultes Personal auch zu halten.

Die Maßnahme: Damit Beratungsstellen im Opferschutz diesen Bedürfnissen auch in Zukunft gerecht werden können, bedarf es einer soliden und nachhaltigen Finanzierung, die eine langfristige Planung ermöglicht. Dabei sollte Opferschutz vor Täterschutz stehen und gerade dieser Gruppe der Betroffenen von digitaler Gewalt der Zugang zu Unterstützung dauerhaft als Teil der Daseinsfürsorge gesichert werden.

HateAid

Die gemeinnützige Organisation HateAid wurde 2018 gegründet und hat ihren Hauptsitz in Berlin. Sie setzt sich für Menschenrechte im digitalen Raum ein und engagiert sich auf gesellschaftlicher wie politischer Ebene gegen digitale Gewalt und ihre Folgen. HateAid unterstützt Betroffene von digitaler Gewalt konkret durch Beratung und Prozesskostenfinanzierung. Die Organisation hat es sich dabei zum Ziel gesetzt, die Strafverfolgung bei Hasskriminalität im digitalen Raum zu stärken. Zu diesem Zweck unterstützt HateAid Menschen, die im Internet in angefeindet werden bei der Strafanzeige. Bereits seit 2019 ist HateAid Mitglied des Bündnisses „Keine Macht dem Hass“, welches vom Hessischen Ministerium der Justiz initiiert wurde. HateAid ist Träger der Theodor-Heuss-Medaille.
