HINWEISE UND MASSNAHMEN ZUR NON-DISKRIMINIERUNG KLEINERER PLATTFORMEN IM RAHMEN DES AKTUELLEN KOMMUNIKATIONSPLATTFORMENGESETZ: UNTERSTÜTZUNGSMODELLE ZUR VERMEIDUNG VON OVERBLOCKING IN DER CYBERGOVERNANCE

Karl Pinter / Dominik Schmelz / Thomas Grechenig

Karl Pinter, TU Wien, Institute of Information Systems Engineering, Research Group for Industrial Software (INSO)
Wiedner Hauptstraße 76/2, 1040 Wien, AT
karl.pinter@inso.tuwien.ac.at; https://www.inso.tuwien.ac.at

Dominik Schmelz, TU Wien, Institute of Information Systems Engineering, Research Group for Industrial Software (INSO)
Wiedner Hauptstraße 76/2, 1040 Wien, AT
dominik.schmelz@inso.tuwien.ac.at; https://www.inso.tuwien.ac.at

Thomas Grechenig, TU Wien, Institute of Information Systems Engineering, Research Group for Industrial Software (INSO)
Wiedner Hauptstraße 76/2, 1040 Wien, AT
thomas.grechenig@inso.tuwien.ac.at; https://www.inso.tuwien.ac.at

Schlagworte: ***KoPl-G, eGovernment, Vorratsdaten, Tracking, DSGVO, Blockchain, Legal Tech***

Abstract: *Das Kommunikationsplattformengesetz richtet sich gegen hetzerische Beiträge im Netz. Betroffene Online Plattformen müssen Möglichkeiten der Meldung und Löschung zur Verfügung stellen. Dabei existiert keine einheitliche Meldestelle. Die Bürgerinnen und Bürger sollen in die Lage versetzt werden, Meldungen gesichert und nachvollziehbar nach einem zentralen Schema vorzunehmen. Den Kommunikationsplattformbetreibern soll es ermöglicht werden, fundierte Entscheidungen treffen zu können, um Overblocking zu vermeiden. Die Autoren schlagen eine Legal Technology, im Sinne von maßvoller Cybergovernance und bürgernahem eGovernment vor.*

1. Einführung und Motivation

Angelehnt an das Netzwerkdurchsetzungsgesetz (NetzDG) in Deutschland, wurden in Österreich Maßnahmen gegen Hass im Netz ergriffen.[1] Das Herzstück der Initiative ist das Kommunikationsplattformengesetz (KoPl-G), das sich zum Zeitpunkt der Drucklegung am Ende der Begutachtungsphase, mit 15.10.2020, befindet. Dabei sind Plattformbetreiber verpflichtet, rechtswidrige Inhalte unter Einhaltung von bestimmten Fristen zu löschen. Die Plattformbetreiber sind durch Größe und Umsatz definiert. Die Inhalte sind bei Eindeutigkeit der Rechtswidrigkeit, selbst für juristische Laien, binnen 24 Stunden zu löschen. Bei uneindeutigen Fällen hat der Plattformbetreiber eine Woche Zeit. Hier setzen die Autoren an, einen Beitrag gegen Overblocking und gegen Hass im Netz zu setzen.

Das deutsche NetzDG steht durchaus unter Kritik, wie man den aktuellen Entscheidungen entnehmen kann.[2]

[1] Bundesministerium für Justiz, Hass im Netz, 2020.

[2] Markert, Raphael, Netz-DG: Vorbild für repressive Regierungen weltweit?, 2020.

1.1. SVN-G

Das „Bundesgesetz über Sorgfalt und Verantwortung im Netz“ (SVN-G) wurde 2019 in Begutachtung geschickt. Das SVN-G hätte zur Folge gehabt, dass definierte Anbieter von Kommunikationsplattformen Sorge tragen hätten müssen, dass die Benutzer mittels „Klarnamenpflicht“, durch Hinterlegung von eindeutigen IDs, leicht ausforschbar gewesen wären. Betroffen gewesen wären Plattformen mit über 100.000 Benutzern, oder 500.000 Euro Umsatz oder Empfänger von mehr als 50.000 Euro an Presseförderung. Hier können bezüglich des Kreises an Betroffenen Parallelen zum KoPl-G gezogen werden. Auch die ursprüngliche Intention ist ähnlich, beide Vorhaben sollten Hass im Netz bekämpfen.

Die Speicherung, im Sinne des SVN-G von persönlichen Daten durch Betreiber von Plattformen, wurde kritisch gesehen, so hätten Vorname, Nachname, Adresse usw. gespeichert und im Falle von Anfragen auch ausgehändigt werden müssen.[3]

Aus mannigfaltigen Gründen wurde das SVN-G daher von Kritikern als eine Form der Vorratsdatenspeicherung wahrgenommen.[4] Die damalige Architektur wurde von den Autoren untersucht und sie konnten zahlreiche Schwachstellen identifizieren.[5]

Ein ähnliches Gesetzesvorhaben, wie das damals geplante SVN-G, wurde bereits 2007 von Südkorea umgesetzt und später wegen verfassungsrechtlichen Bedenken aufgehoben.[6] Diese erfolgte Umsetzung ermöglichte es, Studien über die Auswirkung von Maßnahmen gegen „Hass im Netz“ zu untersuchen, im konkreten Fall durch eine Ausweispflicht der Benutzer von Plattformen. Es zeigte sich, dass das Risiko von Cyberattacken anstieg. Das mag wenig überraschen, denn wertvolle personenbezogene Daten wurden nun von Plattformen gespeichert, die vorher nur über Pseudonyme verfügten.[7] Allerdings wurden auch Veränderungen im Verhalten von Benutzerinnen und Benutzern festgestellt, diese trafen allerdings nicht die intendierte Zielgruppe.[8] Ebenso konnte eine „Flucht“ auf ausländische Plattformen, die nicht dem koreanischen Recht unterworfen waren, beobachtet werden.[9]

1.2. KoPl-G

Der vorliegende Entwurf des KoPl-G stellt auf folgende Anbieter von in- und ausländischen Kommunikationsplattformen ab:

- Ab 100 000 Benutzern (in Österreich)
- Umsatz durch den Betrieb über 500 000 Euro im vorangegangenen Jahr
- Ausnahmen: Vermittlung oder Verkauf von Waren und Dienstleistungen. Medienunternehmen, die journalistisch aufbereitete Inhalte zur Verfügung stellen, sind ebenfalls ausgenommen.

Der Entwurf unterscheidet nicht, ob eine Kommunikationsplattform gewinnorientiert arbeitet. Es wird explizit auf Benutzerinnen und Benutzern aus Österreich abgestellt. Das hat unmittelbar zur Folge, dass jeder Plattformbetreiber die Lokation seiner Registrierten und/oder Benutzerinnen und Benutzer kennen muss. Damit muss die IP Adresse oder GPS Information vorgehalten werden. Während die GPS Information kein

[3] Pinter et al., Towards a Multi-party, Blockchain-Based Identity Verification Solution to Implement Clear Name Laws for Online Media Platforms. Springer International Publishing, 2019.
[4] Hammer, Viele offene Fragen zu Registrierungspflicht, 2020.
[5] Pinter et al., Towards a Multi-party, Blockchain-Based Identity Verification Solution to Implement Clear Name Laws for Online Media Platforms. Springer International Publishing, 2019.
[6] Cho et al., Empirical analysis of online anonymity and user behaviors: the impact of real name policy, 2012.
[7] Ja-Young, Internet real-name system to be scrapped, 2020.
[8] Cho et al., Empirical analysis of online anonymity and user behaviors: the impact of real name policy, 2012, S. 3047.
[9] Ja-Young, Internet real-name system to be scrapped, 2020.

praxistaugliches Mittel darstellt, muss eine Form der Vorratsdatenspeicherung in Form einer Zuteilung von Geolokationen zu IP Adressen vorgenommen werden.[10]

1.3. Betroffene Plattformen

Lohninger («Welche Online-Plattformen vom neuen „Hass im Netz"-Paket betroffen sein werden ») untersuchte, welche Plattformen vom KoPl-G betroffen sind.[11] Identifiziert wurden neben den großen, zumeist amerikanischen Plattformen wie Facebook, auch europäische Anbieter von Datingplattformen oder e-Learninganbieter. Weiters sind Familienplattformen und Plattformen, die kollaboratives Arbeiten ermöglichen, betroffen. Plattformen, um Arbeitgeber zu bewerten befinden sich ebenso wie Crowdfundingplattformen unter den von Lohninger («Welche Online-Plattformen vom neuen „Hass im Netz"-Paket betroffen sein werden») untersuchten Beispielen.

2. Problemstellung

Um eine Analyse zur Verbesserung einer Architektur zu erstellen, wurden von den Autoren folgende kritischen Stellen nach Lohninger et al. («Stellungnahme KoPlG») untersucht:

- Der Anwendungsbereich ist weit gestreut. Damit fällt eine Abgrenzung schwer.[12]
- Es handelt sich um eine Form von Vorratsdatenspeicherung: Die Beweislast bezüglich Benutzerzahlen liegt beim Betreiber.[13] Daher müssen IP Adressen verarbeitet und gespeichert werden.
- Der Begriff „Kommunikationsplattform" ist sehr weit gegriffen.[14]
- Es besteht die Unmöglichkeit für Kommunikationsplattformen über rechtswidrige Inhalte zu entscheiden[15]. Es obliegt privaten Unternehmen zu beurteilen, ob ein rechtswidriger Inhalt vorliegt.
- Aus dem Vorherigen ergibt sich unmittelbar die Gefahr von Overblocking.[16]
- Die Beschwerdeverfahren sind unklar definiert.[17]
- Fixbeträge bei Geldbußen und Geldstrafen im internationalen Kontext erscheinen wenig sinnvoll.[18]

Zusammenfassend kann gesagt werden, dass verhältnismäßig kleine Plattformen aus obigen Gründen zum Overblocking neigen könnten, um Geldbußen und Geldstrafen zu vermeiden. Gleichzeitig sind viele Plattformen betroffen, die nicht über das notwendige Mittel zur Entscheidung über rechtswidrige Inhalte verfügen. Beispielsweise kann nicht festgestellt werden, ob der Vorwurf einer schon abgetanen, gerichtlich strafbaren Handlung erfüllt ist, ohne Einsicht in einschlägige Register zu nehmen.[19] Die Autoren fokussierten sich mit der Ausgestaltung einer Architektur auf die nötige Cybergovernance, mit Hauptaugenmerk auf die Themen Transparenz, Overblocking und Entscheidungsfindung.

[10] Vgl. Lohninger et al., Stellungnahme KoPlG, 2020, S. 4.
[11] Lohninger, Welche Online-Plattformen vom neuen „Hass im Netz"-Paket betroffen sein werden, 2020.
[12] Lohninger et al., Stellungnahme KoPlG, 2020, S. 3.
[13] Ebenda, S. 4.
[14] Ebenda, S. 5.
[15] Ebenda, S. 5.
[16] Ebenda, S. 6.
[17] Ebenda, S. 8.
[18] Ebenda, S. 8f.
[19] Ebenda, S. 5.

2.1. Architektur

Beleuchtet man das geplante KoPl-G auf technische Vorgaben, so findet man große Freiräume in der technischen Ausgestaltung.

Vereinfacht dargestellt (Abbildung 1), ergibt sich folgender Ablauf:

- Eine Posterin oder ein Poster (1) postet Inhalte auf einer vom KoPl-G betroffenen Plattform.
- Eine Einmelderin oder ein Einmelder (2) liest Postings auf jener Plattform.
- Eine Einmelderin oder ein Einmelder meldet mittels vom Betreiber der Kommunikationsplattform bereitgestellten Möglichkeit ein Posting (3) mit potentieller Rechtswidrigkeit ein.
- Der Plattformbetreiber muss bei Beschwerden angemessen reagieren und ernennt einen „verantwortlichen Beauftragten“ (4). Gegebenenfalls wird eine Löschung unter Wahrung bestimmter Fristen durchgeführt (5).

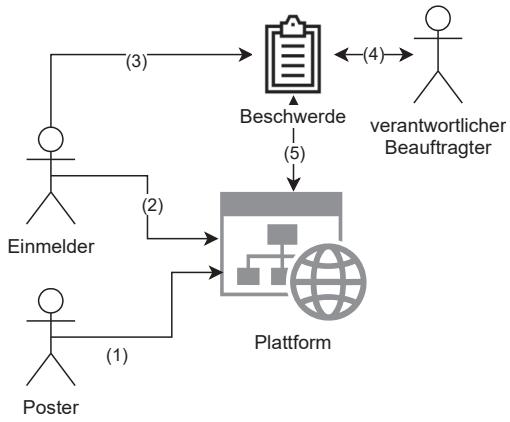

Abbildung 1: KoPl-G

Alle vorliegenden Daten werden vom Plattformbetreiber gespeichert und verwaltet. Daten, die der Benutzeridentifizierung dienen, müssen vorgehalten werden. Der Beschwerdeprozess ist auf jeder Kommunikationsplattform unterschiedlich ausgestaltet. Es gibt keine Instanz, die über den Prozess wacht und diesen dokumentiert, das Beschwerdeverfahren wird von privaten Unternehmen durchgeführt. Für die Benutzerin oder den Benutzer ist das Level an Datenschutz und Datensicherheit nicht ersichtlich.

2.2. Rollen

Die für den vorliegenden Prototypen technisch relevanten Rollen im KoPl-G sind:

- Posterin oder Poster: liest und postet auf einer vom Diensteanbieter betriebenen Plattform.
- Einmelderin oder Einmelder: Kann auch Posterin oder Poster sein. Meldet potenziell rechtswidrige Inhalte.
- Diensteanbieter einer Kommunikationsplattform: betreibt die Plattform und ist verantwortlich. Muss nicht notwendigerweise die technische Basis zur Verfügung stellen. Muss für ein transparentes Verfahren sorgen. Nennt einen „verantwortlichen Beauftragten“.
- Verantwortlicher Beauftragter: Stellt die Einhaltung der Vorschriften des KoPl-G sicher. Wird der Aufsichtsbehörde gemeldet, und muss für diese ständig erreichbar sein.

- Aufsichtsbehörde: Diensteanbieter von Kommunikationsplattformen haben der Aufsichtsbehörde alle relevanten Auskünfte zu erteilen.
- Compliance Organ: Ist nicht notwendigerweise ident mit dem „verantwortlichen Beauftragten". Im Falle des vorgestellten Prototyps ist das Compliance Organ eine einschlägig gebildete Fachkraft, die über die Rechtswidrigkeit von Postings nach einer Meldung entscheidet. Das Compliance Organ bei der prototypischen Umsetzung wird typischerweise kommerzielle Interessen verfolgen.

Diensteanbieter mit über einer Million Benutzer haben der Aufsichtsbehörde Berichte turnusmäßig vorzulegen. Digitale Ausweiskontrollen bei der Registrierung auf einer Plattform sind durch das KoPl-G keine gefordert. Damit kann die wahre Identität von Benutzerinnen oder Benutzern, die Inhalte erstellen (Posterinnen oder Poster), weiterhin mit relativ geringem technischen Aufwand wie TOR, Nutzung von öffentlichen Zugängen, Proxys[20], oder Einsatz von VPNs verschleiert werden.[21]

2.3. Ziele und Anforderungen an einen Prototyp

Bei der Entwicklung eines Prototyps wurden folgende Eckpfeiler eingearbeitet:

- Meldung eines potenziellen Hasspostings über ein einheitliches Meldeverfahren (Wiedererkennung)
- Dokumentation aller Schritte und Persistierung von Prüfwerten auf einer Blockchain (Transparenz und Nachvollziehbarkeit)
- Datenschutzkonforme Betreibbarkeit im Speziellen unter Berücksichtigung von:
  - privacy by design, und
  - privacy by default
- Handeln im Sinne des EU Action Plan[22]:
  - Digital by default: Alle Schritte sind digital durchführbar.
  - Once only Prinzip: Die Meldung erfolgt mittels Meldebutton einmal, danach gelangt die Benutzerin oder der Benutzer zur Dateneingabe. Das Prinzip der Datensparsamkeit ist sichergestellt.
  - Inklusion und Barrierefreiheit: Ein einheitliches System erfüllte einschlägige WAI Kriterien.[23]
  - Offenheit und Transparenz: Wie im KoPl-G gefordert, wird Transparenz geschaffen, alle Verfahrensschritte können zentral verfolgt werden.
  - Standardmäßig grenzübergreifend: Das System kann mittels Schnittstellen an weitere Dienste angebunden werden.
  - Standardmäßig interoperabel
  - Vertrauenswürdigkeit und Sicherheit: Ein offenes System schafft Vertrauen.
- (freiwillige) Nutzung der Bürgerkartenarchitektur und den damit verbundenen Eigenschaften[24]
- Nachvollziehbarkeit und Transparenz gegenüber allen Beteiligten

Ein Problem der Praxis ist eine zuverlässige Erkennung von rechtswidrigen Inhalten, diese kann nicht mittels rein technischer Maßnahmen sichergestellt werden. Daher haben die Autoren die Rolle des Compliance Organs eingeführt. Es handelt sich um eine einschlägig geschulte Person, die fachlich in der Lage ist, die Rechtswidrigkeit zu beurteilen.

---

20 Choi et al., Understanding the Proxy Ecosystem: A Comparative Analysis of Residential and Open Proxies on the Internet, 2020.

21 Ding et al., Effective Methods to Avoid the Internet Censorship, Fourth International Symposium on Parallel Architectures, Algorithms and Programming, Tianjin, 2011.

22 EU-eGovernment-Aktionsplan 2016–2020, 2016.

23 W3C Web Accessibility Initiative, Making the Web Accessible, 2020.

24 Vgl. Kotschy, Die Bürgerkarte in Österreich, Datenschutz und Datensicherheit – DuD, 2006.

3. Prototyp

Die Autoren entwickelten einen Prototyp, um die Machbarkeit der vorgeschlagenen Technik zu demonstrieren (Abbildung 2).

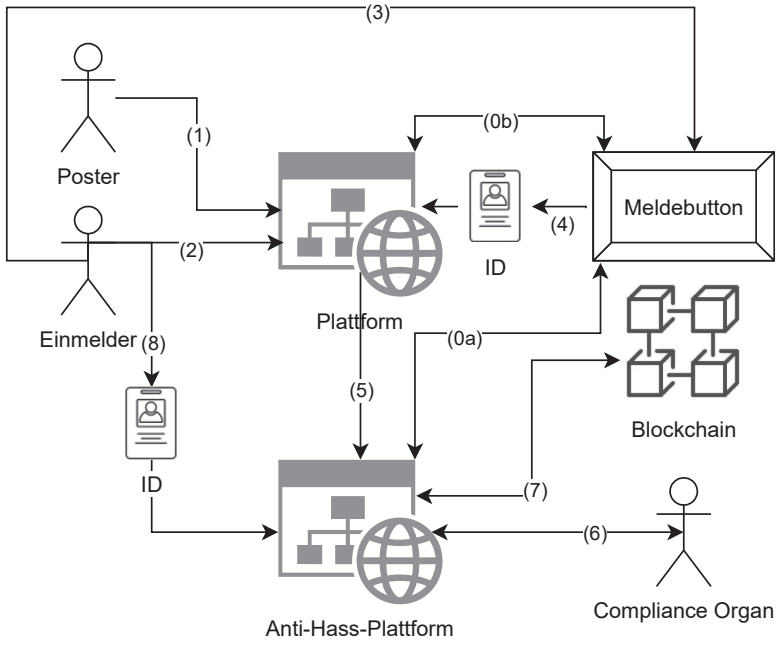

Abbildung 2: Prototyp

Eine dem KoPl-G unterworfene Kommunikationsplattform bindet einen „Meldebutton" (0b), vergleichbar mit dem von Facebook bekannten „Like" Button[25], jedoch mit völlig anderem Datenschutzlevel und Intention, mittels eines von der „Anti-Hass-Plattform" zur Verfügung gestellten Scripts (0a) ein. Eine Posterin oder ein Poster erstellt einen potenziell rechtswidrigen Inhalt (1). Eine Einmelderin oder Einmelder (2) liest Postings auf einer Kommunikationsplattform, die dem KoPl-G unterworfen ist. Es kommt zu einer Einmeldung durch einen Einmelder oder eine Einmelderin (3), weil ein potentiell rechtswidriger Inhalt erkannt wurde. Die Kommunikationsplattform übermittelt an die „Anti-Hass-Plattform" (4):

- ID des Inhalts
- Link zum Inhalt
- Betroffener Inhalt
- Signatur über alle Punkte

Nach der Übermittlung steht der Einmelderin oder dem Einmelder auf der „Anti-Hass-Plattform" die Möglichkeit offen, die Einmeldung zu kommentieren. Mindestens muss eine Begründung der Einmeldung angegeben werden und eine Authentifizierung vorgenommen werden. Die Authentifizierung kann durch die Bürgerkartenarchitektur (4 und 8) erfolgen, oder über herkömmliche Verfahren, wie z.B. Ausweis-Upload. Durch das Einmelden wird ein Beschwerdehash auf der Blockchain persistiert (7). Dieser Wert lässt sich nicht auf die Beschwerde rückführen, kann jedoch im Nachhinein als Beweis der Beschwerde und des Zeitpunktes dieser herangezogen werden. Die Einmelderin oder der Einmelder kann nun mittels der „Anti-Hass-Platt-

[25] Schleipfer, Facebook-Like-Buttons, Datenschutz und Datensicherheit – DuD, 2014.

form“ den Status seiner Einmeldung jederzeit verfolgen (8). Der Status ändert sich von „eingemeldet“, über „in Prüfung“, bis hin zu „nicht akzeptiert“ oder „akzeptiert“.

Ein Kommunikationsplattformbetreiber erhält im Dashboard eine neue Einmeldung und wird über diese benachrichtigt. Ein Laie kann diese bestätigen und manuell eine Löschung oder Sperrung in seiner Plattform vornehmen, oder die Einmeldung an ein Compliance Organ (6) weiterleiten. Dieses kann über das Dashboard dieselben Inhalte bewerten und mit einer Begründung eine Löschung empfehlen. Die Sperrung der Inhalte obliegt immer dem Kommunikationsplattformbetreiber. Das von Lohninger et al. («Stellungnahme KoPlG») angeführte Problem, dass private Unternehmen die Rolle von Gerichten übernehmen könnten, wird damit nicht ausgeschaltet, kann jedoch durch den Einsatz von fachkundigen Compliance Organen (6) mit einschlägiger Ausbildung im Datenrecht abgefedert werden. Das Compliance Organ ist beratend für die der KoPl-G unterworfenen Plattform tätig und gibt eine Einschätzung ab, ob eine Löschung vorgenommen werden soll oder löscht in deren Auftrag. Die Aufsichtsbehörde wurde aus Gründen der Übersichtlichkeit bewusst nicht skizziert.

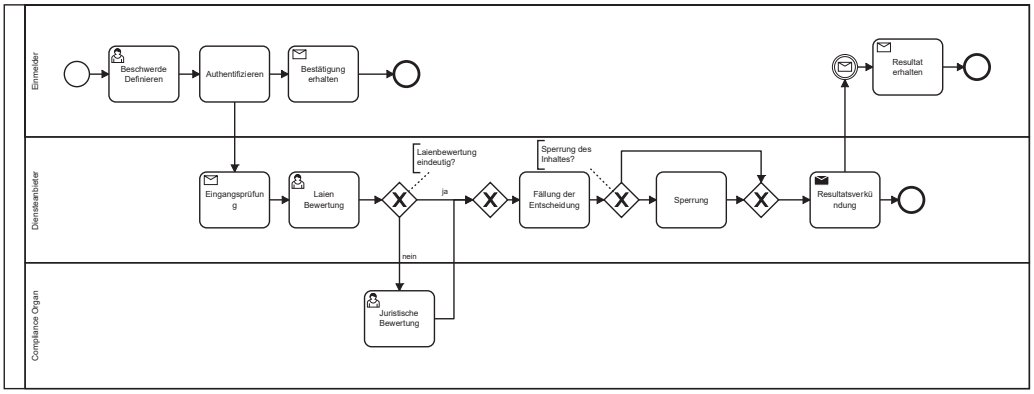

Abbildung 3: Prototyp als Business Prozess

Abbildung 3 stellt den Vorgang als Business Prozess dar, welcher die Rollen „Einmelder“, „Diensteanbieter“ und „Compliance Organ“ und ihre Aufgaben in den Vordergrund stellt. Der „Einmelder“ besucht per „Meldebutton“ die „Anti-Hass-Plattform“, definiert eine Beschwerde und muss sich authentifizieren. Wird die Beschwerde erfolgreich erstellt, bekommt die Einmelderin oder Einmelder eine Bestätigung der Beschwerde via E-Mail inkl. Hash, welcher auf der öffentlichen Blockchain mit Zeitstempel abgelegt wurde.

Der „Diensteanbieter“ erhält eine neue Beschwerdebenachrichtigung per E-Mail und kann diese in der „Anti-Hass-Plattform“ einsehen und eine Eingangsprüfung vornehmen. Ist die „Laien Bewertung“ der Beschwerde eindeutig, so wird direkt eine Entscheidung getroffen, sonst wird das „Compliance Organ“ über die Plattform benachrichtigt und kann über diese Einsicht nehmen und eine Bewertung im Auftrag vornehmen. Jedenfalls, fällt der Diensteanbieter eine Entscheidung, welche als „Resultatsverkündung“ an den Einmelder gesendet wird. Die tatsächliche Löschung des Postings und Benachrichtigung des Urhebers wird nicht durch die „Anti-Hass-Plattform“ durchgeführt.

3.1. Authentifizierung und Begründung

Wenn eine Einmelderin oder ein Einmelder den „Meldebutton“ verwendet, so muss eine Begründung für den Betreiber der Kommunikationsplattform und gegebenenfalls für das Compliance Organ eingegeben werden. Ist die Rechtswidrigkeit bereits für Laien erkennbar, so wird keine einschlägig gebildete Fachkraft mit dem Fall befasst werden und es wird rasch zu einer Löschung kommen, wie im Entwurf des KoPl-G vorgesehen. Bei komplexeren Fällen besteht eine Frist von einer Woche, innerhalb derer gehandelt werden muss. Um die

Abläufe schlank zu halten, kann eine Authentifizierung mittels Bürgerkarte vorgenommen werden. Alternativ ist ein Ausweis Upload möglich. Abbildung 4 zeigt einen Screenshot des Prototyps.

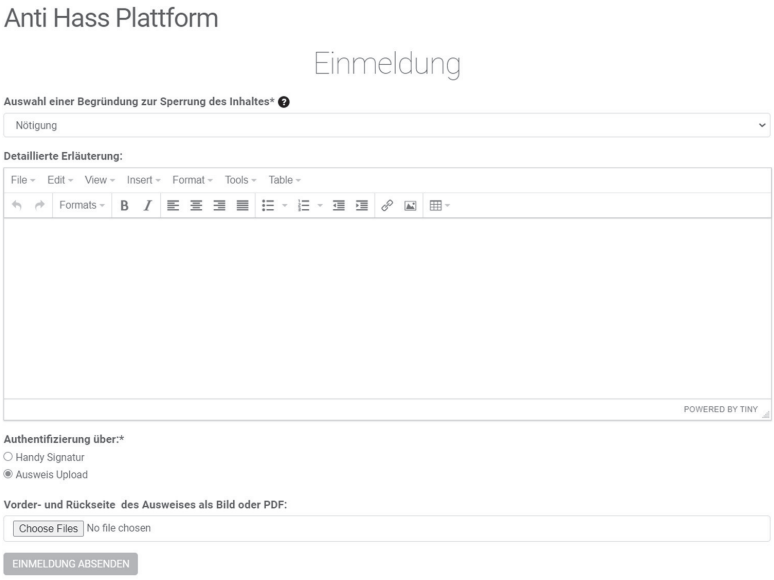

Abbildung 4: Einmeldung

3.2. Dashboard

Das Dashboard, siehe Abbildung 5, ist eine gesammelte Ansicht von Einmeldungen inklusive Status und Kurzinformation, mit der Möglichkeit, in eine Detailansicht je Einmeldung zu wechseln. Je nach Rolle („Einmelder“, „Diensteanbieter“ und „Compliance Organ“), können unterschiedliche Informationen eingesehen, und Aktionen durchgeführt werden.

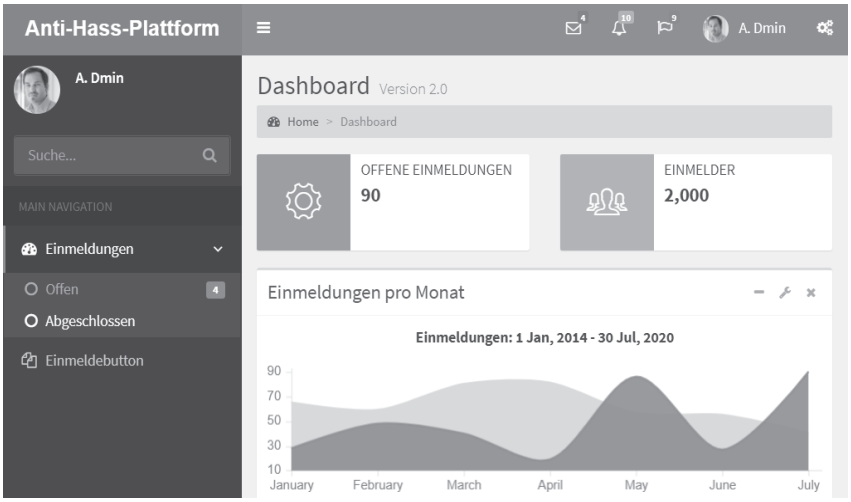

Abbildung 5: Dashboard

Eine Einmelderin oder ein Einmelder kann mehrere Postings, auch auf verschiedenen Plattformen, einmelden. Die Dokumentation der Einmeldungen läuft gesammelt im Dashboard der „Anti-Hass-Plattform" zusammen. Die Einmelderin oder der Einmelder können dort jederzeit Einsicht in den jeweiligen Status nehmen. Damit ist auch der im Entwurf geforderte Transparenzauftrag erfüllt.

Ein „Dienstanbieter", siehe Abbildung 5, sieht nach dem Login eine grafische Darstellung der Einmeldungen pro Monat und die Anzahl der offenen Einmeldungen, welche noch bearbeitet werden müssen. In einer weiteren Darstellung („Einmeldungen" – „Offen") sieht der „Diensteanbieter" die noch zu bearbeitenden Einmeldungen, sortiert nach Dringlichkeit der Bearbeitung (verbleibende Restzeit und Art der Beschwerde). In der Detailansicht kann die Beschwerde bearbeitet bzw. dem „Compliance Organ" weitergegeben werden.

Das „Compliance Organ" hat eine ähnliche Ansicht, welche die weitergegebenen Beschwerden übersichtlich darstellt. In der Detailansicht ist eine chronologische Detaildarstellung der Informationen zu einer Beschwerde bzw. einem Inhalt ersichtlich. Dadurch ist es dem „Compliance Organ" möglich eine fundierte Entscheidung zu treffen.

4. Schlussfolgerungen

Wie das Beispiel SVN-G und Südkorea zeigte, sind Gesetze gegen Hass im Netz nicht immer praxistauglich umsetzbar. Eine schonende Umsetzung der Klarnamenpflicht wäre mit entsprechendem technischen Aufwand möglich.[26] Die Klarnamenpflicht hat sich nicht bewährt, dies wurde auch vom Gesetzgeber erkannt und entsprechende Passagen finden sich im KoPl-G nicht.

Setzt man das KoPl-G in der vorliegenden Fassung um, so bleibt jedem Betreiber überlassen, wie die konkrete technische Ausgestaltung auszusehen hat. Die Autoren zeigen, dass eine einheitliche und automatisierte Abwicklung mittels Meldebutton möglich ist. Damit entsteht für alle Stakeholder ein Mehrwert, im Sinne von Transparenz und Rechtssicherheit. Eine Einmelderin oder ein Einmelder von einem potenziellen Hassposting hat die Möglichkeit, alle Schritte im Dashboard zu verfolgen. Diese Logs sind unveränderlich dokumentiert und im Falle von weiteren Schritten damit auch sicher dokumentiert. Den Betreiber von Plattformen wäre mit dem Einsatz von Compliance Organen geholfen, die eine fachkundige Einschätzung bezüglich der möglichen Rechtswidrigkeit abgeben können. Dabei kann sich die „Anti-Hass-Plattform" entweder auf Freiwilligkeit oder auf kommerzielle Mitarbeiterinnen und Mitarbeiter stützen, die seriöses Feedback an die Plattformbetreiber zurückmelden.

5. Literatur

Bundesministerium für Justiz, Hass im Netz, BMJ, https://www.bmj.gv.at/themen/gewalt-im-netz.html (aufgerufen am 03. September 2020), 2020.

Cho, D./Kim, S./Acquisti, A., Empirical analysis of online anonymity and user behaviors: the impact of real name policy, 45th Hawaii International Conference on System Sciences, 2012, S. 3041-3050.

Choi, J. et al., Understanding the Proxy Ecosystem: A Comparative Analysis of Residential and Open Proxies on the Internet, IEEE Access, vol. 8, 2020, S. 111368-111380.

Ding, F./Yang, Z./Chen, X./Guo J., Effective Methods to Avoid the Internet Censorship, Fourth International Symposium on Parallel Architectures, Algorithms and Programming, Tianjin, 2011, S. 67–71.

Hammer, Dominique, Viele offene Fragen zu Registrierungspflicht, ORF, https://orf.at/stories/3118452/ (aufgerufen am 10. Oktober 2020), 2020.

Ja-Young, Yoon, Internet real-name system to be scrapped, Korea Times, http://www.koreatimes.co.kr/www/news/biz/2013/08/602_101841.html (aufgerufen am 28. September 2020), 2020.

[26] Pinter et al., Towards a Multi-party, Blockchain-Based Identity Verification Solution to Implement Clear Name Laws for Online Media Platforms, 2019.

Kotschy, Waltraud, Die Bürgerkarte in Österreich, Datenschutz und Datensicherheit – DuD, 2006, Heft 30.4, S. 201–206.

Lohninger, Thomas/Asiemo, Nicola, Stellungnahme KoPlG, epicenter.works, https://epicenter.works/sites/default/files/epicenter.works_-_koplg-netzdg.pdf (aufgerufen am 17. Oktober 2020), 2020.

Lohninger, Thomas, Welche Online-Plattformen vom neuen „Hass im Netz"-Paket betroffen sein werden, epicenter.works, https://epicenter.works/content/welche-online-plattformen-vom-neuen-hass-im-netz-paket-betroffen-sein-werden (aufgerufen am 16. Oktober 2020), 2020.

Markert, Raphael, Netz-DG: Vorbild für repressive Regierungen weltweit?, Süddeutsche Zeitung, https://www.sueddeutsche.de/digital/netz-dg-internetzensur-facebook-1.4840302 (aufgerufen am 27. September 2009), 2020.

Mitteilung der Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen, EU-eGovernment-Aktionsplan 2016–2020, https://eur-lex. europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:52016DC0179&from=EN (aufgerufen am 22. August 2020), 2016.

Pinter, Karl/Schmelz, Dominik/Lamber, René/Strobl, Stefan/Grechenig, thomas, Towards a Multi-party, Blockchain-Based Identity Verification Solution to Implement Clear Name Laws for Online Media Platforms. In: DiCiccio, Claudio/Gabryelczyk, Renata/García-Bañuelos, Luciano/Hernaus, Tomislav/Hull, Rick/Indihar Štemberger, Mojca/Kő, Andrea/Staples, Mark (Hrsg.), Business Process Management: Blockchain and Central and Eastern Europe Forum, Springer International Publishing, Switzerland, 2019, S. 151–165.

Schleipfer, Stefan, Facebook-Like-Buttons, Datenschutz und Datensicherheit – DuD, 2014, Heft 38, S. 318–324.

W3C Web Accessibility Initiative, Making the Web Accessible, W3C, https://www.w3.org/WAI/ (aufgerufen am 24. September 2020), 2020.