... changing the digital world together!

Digital Society
Graben 17/10
1010 Wien

+43 1 314 40-0
Info@DigiSociety.ngo

An:

team.z@bmj.gv.at

team.s@bmj.gv.at

medienrecht@bka.gv.at

begutachtungsverfahren@parlament.gv.at

Wien, 15.10.20

Betreff: Stellungnahme zu den Ministerialentwürfen des Pakets "Hass-im-Netz", HiNBG, 48/ME XXVII. GP, GZ 2020.0.479.295; 50/ME XXVII. GP, GZ 2020-0.554.389; KoPl-G, 49/ME XXVII. GP, GZ 2020-0.452.909

Sehr geehrte Damen und Herren,

Die Digitalisierung unserer Gesellschaft bringt umwälzende Veränderungen für die gesamte Gesellschaft. Die ***Digital Society*** ist ein unabhängiger und gemeinnütziger Verein. Wir beschäftigen uns mit den Auswirkungen dieser Veränderungen auf die Gesellschaft, analysieren diese gemeinsam mit Expert:innen und erarbeiten politische Lösungen für aktuelle gesellschaftliche Probleme. Die geplante Novelle ist sehr begrüßenswert, enthält aber eine ganze Reihe von impliziten technischen Problem-stellungen. Wir haben diese analysiert und übersenden unsere Ergebnisse und Vorschläge für die obengenannten drei Entwürfe in den nachfolgenden drei Hauptkapiteln.

Stellungnahme zu HiNBG, 48/ME XXVII. GP, GZ 2020.0.479.295

Link zu den Materialien:

https://www.parlament.gv.at/PAKT/VHG/XXVII/ME/ME_00048/index.shtml

§ 17a Abs. 2 ABGB unklar

Der vorgeschlagene zweite Satz lautet:

> *"Soweit gesetzlich nichts anderes bestimmt ist und soweit nicht eine zulässige kommerzielle Verwertung des Persönlichkeitsrechts im Vordergrund steht, kann die Einwilligung nur vom entscheidungsfähigen Träger des Persönlichkeitsrechts selbst erteilt werden."*

Dies könnte so interpretiert werden, dass jede kommerzielle Verwendung eines Persönlichkeitsrechts zulässig ist, wenn nicht explizit verboten. Erst in den Materialien wird klargestellt, dass hier nur der vermögensrechtlichen Teil der Persönlichkeitsrechte gemeint ist. Dies sollte in den Gesetzestext einfließen. Wir schlagen vor, den Satz wie folgt zu formulieren:

> *"Die Einwilligung zu einem Eingriff kann nur vom entscheidungsfähigen Träger des Persönlichkeitsrechts selbst erteilt werden, ausgenommen in gesetzlich definierten Fällen. Rechte, die sich ausschließlich auf einen vermögens-rechtlichen Teil des Persönlichkeitsrechts beziehen, können nach den privatrechtlichen Regeln auch unabhängig von einer Einwilligung übertragen werden."*

§ 20 Abs 3 ABGB beinhaltet Netzsperren und Uploadfilter

Die Konstituierung eines Unterlassungsanspruchs auch gegenüber einem Vermittler führt im Digitalen Raum logisch zwingend zu Netzsperren und Netzfiltern, wie im Folgenden gezeigt wird.

Netzsperren und Uploadfilter sind keine geeigneten Mittel zur Durchsetzung von Unterlassungsansprüchen

Handlungen im Digitalen Raum passieren automatisch und autonom, sie werden zwar durch menschlichen Willen angestoßen, können jedoch danach nur mehr mit aufwendigem Einsatz menschlicher Zeit überwacht werden. Die Übermittlung von Daten oder das Veröffentlichen von Informationen durch Vermittler geschehen dort vollautomatisch, ohne dass es beim Vermittler eine Person gibt, auf die sich ein Unterlassungsanspruch beziehen könnte.

Zur Durchsetzung müsste man entweder künstlich wieder Personen in den Prozess einfügen, die die automatischen Abläufe auf die Einhaltung der Unterlassung prüfen - was sich durch die schiere Menge verbietet - oder entsprechende technische Maßnahmen in Form von Netzsperren und Uploadfiltern setzen.

Wie in der Vergangenheit schon wiederholt argumentiert wurde sind Netzsperren technisch ungeeignet, um eine solche Unterlassung durchzusetzen. Die Digitale Welt ist auf Grund ihrer Vernetztheit sehr robust gegenüber punktuellen Eingriffen, und ihre Grenzenlosigkeit macht es zu einem unmöglichen Unterfangen, einen national bestehenden Rechtsanspruch auf Unterlassung international durchzusetzen.

Auch Uploadfilter stoßen schnell an Grenzen. Ein Unterlassungsanspruch bezieht sich auf einen bestimmten (Gedanken)Inhalt, der nicht mehr verbreitet werden darf. Technische Maßnahmen wie Filter sind jedoch stark an die Form der Verbreitung gebunden. Eine Beleidigung beispielsweise kann in unterschiedliche Worte gefasst werden, sie kann als Text oder in Form eines Bildes übertragen werden. Die Vielfalt der Möglichkeiten schließt hier eine mit vertretbarem Aufwand machbare technische Lösung aus. Einfache technische Lösungen wiederum sind nicht effektiv.

Auch ist an dieser Stelle auf die Grundrechtsproblematik hinzuweisen. Falsch gesetzte Netzsperren oder zu breit definierte Filter können gegebenenfalls in das Recht auf freie Meinungsäußerung dritter unbeteiligter Personen eingreifen.

§549 ZPO ist zu begrüßen, aber...

Begrüßenswert ist ein rascher Zugang zu einer Möglichkeit, verletzende Inhalte aus dem Netz zu entfernen. Problematisch ist aber auch hier der implizit enthaltene Unterlassungsanspruch gegenüber Vermittlern, da auch dies zu Netzsperren und Uploadfiltern(siehe oben) führt. Ein Take-Down-Anspruch gegenüber Vermittlern ist zweifellos notwendig, für einen Stay-Down-Anspruch sollte aber primär nur der Täter in Anspruch genommen werden. Dies wäre explizit zu vermerken.

§59 JN: Fixer Streitwert problematisch

Der fixe Streitwert von 5000€ erscheint problematisch. Er mag in Standardfällen gerechtfertigt sein, kann aber in individuellen sehr schweren Fällen zu niedrig sein.

Eine Ergänzung um

> "*Der Nachweis eines höheren Streitwerts ist möglich*"

erscheint sinnvoll. Ein solcher Nachweis würde sich an der wirtschaftlichen Person des Opfers sowie an der Größe der Verbreitung der Nachricht und den Folgen der Verbreitung orientieren und damit der unterschiedlichen Größe der Kommunikationsplattformen Rechnung tragen.

getting you ready for tomorrow!
Digital Society | Graben 17/10 | 1010 Wien
ZVR: 547238411 | https://DigiSociety.ngo

Stellungnahme zu 50/ME XXVII. GP, GZ 2020-0.554.3895

Link zu den Materialien:

https://www.parlament.gv.at/PAKT/VHG/XXVII/ME/ME_00050/index.shtml

§ 120a StGB hat Lücken hinsichtlich des geschützten Bereichs

Die Aufnahme dieses Tatbestands in das StGB ist ein wichtiger Schritt, um der Weiterentwicklung der Technologie Rechnung zu tragen. Handykameras sind mittlerweile allgegenwärtig und stellen durch ihre Vernetztheit eine zunehmende Bedrohung für die Privatsphäre dar.

Die vorgeschlagene Regelung, die sich erkennbar gegen Up-Skirting richtet, ist an einigen Stellen zu eng gefasst. Die Beschränkung auf Bedeckung durch Textilien erscheint willkürlich, es sollte egal sein, durch welches Material oder welchen Gegenstand ein Einblick verwehrt wird. Auch ist nicht klar, ob eine Wohnung mit offenen Fenstern unter den Begriff des geschützten Raums fällt (was sie tun sollte).

Die Begriffswahl des Paragraphen zielt eindeutig auf einen sexualisierten Kontext hin. Es gibt aber auch Fälle wie beispielsweise Unfallopfer, die einen entsprechenden Schutz vor reißerischen Bildaufnahmen benötigen. Auch das Beobachten und Fotografieren von Menschen mittels Teleobjektiv an einem menschenleeren Stand oder in der eigenen Wohnung sollte entsprechend geschützt sein, da auch dies tief in die Privatsphäre eingreift.

Die technologische Entwicklung ermöglicht zudem auch Aufnahmen in anderen Frequenzbereichen als dem sichtbaren Licht, mit ähnlichen Problematiken. Infrarotaufnahmen können durch dünne Kleidung hindurchsehen. Die neuesten Nackt-Scanner-Technologien, wie sie als Sicherheitsmaßnahmen an Flugplätzen schon zum Einsatz kommen, werden in absehbarer Zeit im Preis fallen und dadurch mehr Verbreitung im privaten Berecht erhalten.

Abstrahiert man all diese Fälle, so geht es um Situationen, in denen eine Person eine gewisse Erwartung von Privatsphäre haben kann, weil sie sich in einem geschützten Raum befindet; weil sie nicht damit rechnen muss, dass ihre Situation im Moment bildlich aufgezeichnet wird (menschenleerer Strand); weil sie Vorkehrungen gegen entsprechende Aufnahmen getroffen hat (Bekleidung), die jedoch durch Technologie wie eine kleine Handykamera, die problemlos unter einen Rock gehalten werden kann, oder ein weitreichendes Teleobjektiv zunichte gemacht werden.

Der Paragraph stellt einen wichtigen ersten Schritt dar, für die Zukunft sollte aber überlegt werden, ob nicht besser die Privatsphäre allgemein als zu schützendes

getting you ready for tomorrow!
Digital Society | Graben 17/10 | 1010 Wien
ZVR: 547238411 | https://DigiSociety.ngo

Rechtsgut herzunehmen wäre statt einer sexualisierten Intimsphäre, auch wenn dies einer der Hauptanwendungsbereiche ist.

Die Strafdrohung erscheint hoch. Da das Strafrecht nur Ultima Ratio sein sollte, wäre zu überlegen, die Strafbarkeit auf grobe Verstöße zu begrenzen, was zugegeben schwierig ist, oder den Paragraphen doch eher aus dem Primärstrafrecht in das Verwaltungsstrafrecht zu verschieben. Auf jeden Fall sollte zwischen dem bloßen Anfertigen und der Weiterverbreitung solcher Fotos in der Strafhöhe unterschieden werden. Eine Verbreitung kann für das Opfer zweifellos weitaus unangenehmer sein.

Abschließend ist darauf hinzuweisen, dass der Straftatbestand besser als Ermächtigungsdelikt zu gestalten ist, da wohl nur das Opfer einschätzen kann, inwieweit eine Verfolgung aus seiner Sicht sinnvoll und wünschenswert ist, Stichwort sekundäre Viktimisierung.

§7a Abs 1 MedienG: Fehlender Schutz für nahe Angehörige von Verstorbenen

Hier wird von Personen gesprochen, die Opfer von Beeinträchtigungen geworden sind. Somit sind Verstorbene nicht mitgemeint. §7a sollte dahingehend erweitert werden, dass der Schutz auch verstorbenen Opfern bzw. deren nahen Angehörigen zugute kommt. In der derzeitigen Formulierung wäre es möglich, die Identität von Todesopfern preiszugeben, was jedoch auch implizit die nahen Angehörigen mit dem Todesfall in Verbindung bringt.

Formulierungsvorschlag:

> "... *und werden dadurch schutzwürdige Interessen dieser Person* ***oder deren nahen Angehörigen*** *verletzt, so haben* ***die Betroffenen*** *Anspruch ...*"

Analoges gilt für § 7b Abs 1.

Auch für die §§ 6 und 7 sollte erwogen werden, inwieweit der Schutz auch nahen Angehörigen von Verstorbenen zukommen soll.

§71 StPO Missbrauchsgefahr hinsichtlich Datenschutz

Begrüßenswert ist, dass die Beweiserhebung inklusive Ausforschung des Täters bei Privatanklagedelekten durch staatliche Stellen erfolgen soll, die hohen Sicherheitskriterien unterliegen.

Es sollte jedoch explizit festgelegt werden, dass die Weitergabe dieser Ermittlungsergebnisse erst im Rahmen einer tatsächlichen Anklageerhebung des Opfers erfolgen darf (und nicht schon im Vorfeld), da sich sonst eine Datenschutz-Lücke und somit Missbrauchspotential auftut. Privatpersonen könnten sonst

Ermittlungsverfahren anstoßen, dann jedoch nach Vorliegen der Ermittlungsergebnisse auf eine weitere Anklage verzichten und somit Kenntnis von persönlichen Daten erlangen.

Stellungnahme zu KoPl-G, 49/ME XXVII. GP, GZ 2020-0.452.909

Link zu den Materialien:

https://www.parlament.gv.at/PAKT/VHG/XXVII/ME/ME_00049/index.shtml

§ 1 Abs 2 KoPl-G; Anwendungsbereich zu weit gefasst

Die Verknüpfung von Benutzer:innenzahlen und Umsatz ist problematisch. Während es klar ist, dass Plattformbetreiber:innen mit entsprechend hohem Umsatz auch entsprechend in die Verantwortung genommen werden können, kostenspielige händische Überprüfungen von Meldungen durchzuführen, ist dies bei den reinen Nutzer:innenzahlen nicht einzusehen. Hier würden gemeinnützige, nicht auf Gewinn ausgerichtete Plattformbetreiber:innen stark behindert. Sie müssten ihre Nutzer:innenzahl limitieren, um ausserhalb des Anwendungsbereichs des Gesetzes zu bleiben. Dies behindert vor allem Newcomer am österreichischen Markt.

§ 1 Abs 2 Z 1 KoPl-G: Problematische Feststellung der Nationalität der Benutzer:innen

Hinter dem harmlos klingenden Begriff "*Nutzer in Österreich*" steckt eine erhebliche technische Hürde. Die Identität der Benutzer:innen wird im Allgemeinen auf den Kommunikationsplattformen nicht näher erhoben, es genügt meist eine E-Mail-Adresse zur Anmeldung, die keinen Rückschluss auf das Ursprungsland zulässt. Eine Angabe des Wohnorts ist freiwillig und Falschangaben können nicht ohne weiteres entdeckt werden. Eine Zuordnung über die IP-Adresse ist rechtlich problematisch, da es sich hier um ein personenbezogenes Datum handelt. Auch ist diese Methode der Herkunftsfeststellung auch nicht besonders zuverlässig, da zunehmend Netzwerkzugänge über VPNs in anderen Ländern erfolgen, beispielsweise bei Mitarbeiter:innen von internationalen Konzernen.

Auch ist nicht klar, wie hier "*in*" zu interpretieren ist. Sind nur Personen gemeint, die ihren regulären Wohnsitz in Österreich haben? Was ist mit Personen, die normalerweise im EU-Ausland wohnhaft sind, sich zeitweise in Österreich aufhalten und von hier aus die Kommunikationsplattform verwenden? Zählen diese hinzu?

Hier bedarf es dringend einer genaueren Definition für eine bessere Rechtssicherheit.

§ 1 Abs 3 KoPl-G: Ausnahmen laden zur Umgehung ein

Die Ausnahmen für Vermittlungs- und Verkaufsplattformen sowie für Medienunternehmen erscheinen willkürlich. Es liegt nicht an der Art des Drumherums, ob die Kommunikation auf einer Plattform anfällig für Hass ist.

Würde Facebook beispielsweise beginnen, redaktionellen Kontent auf der Startseite einzublenden, könnte es sich als Medienunternehmen bezeichnen und würde, ohne dass sich etwas an der Hassproblematik unter den Benutzer:innen ändert, aus dem Geltungsbereich des Gesetzes herausfallen.

Genauso absurd ist es, dass Amazon aus dem Geltungsbereich heraus fällt, wo es in den Kommentaren zu Produkten durchaus zu Diskussionen und auch oft genug zu Hasspostings kommt, dass Amazon in den Benutzerrichtlinien diesbezüglich sehr detaillierte Regeln aufstellen musste.

§ 3 KoPl-G: Überschießende Blockierungen müssen vermieden werden

Derzeit beschäftigt sich das Gesetz nur mit der Problematik, Hasspostings zügig aus dem Netz zu entfernen. Es gibt jedoch auch den gegenteiligen Fall, wo durch fälschliches Melden als Hassposting normale, aber unliebsame Postings zensuriert werden sollen. Solche Fälle greifen in die Redefreiheit ein und müssen daher auch behandelt werden. Wird nur das Nicht-Entfernen von Hasspostings pönalisiert, so besteht die Gefahr eines Über-Blockierens durch die Platformbetreibenden, was einem demokratischen Diskurs nicht gut tut. Hier braucht es entsprechende Regulierungen, die auch ein überschießendes Blockieren in irgendeiner Form pönalisieren (und sei es nur durch einen erhöhten Dokumentationsaufwand).

§ 3 Abs 3 KoPl-G zu unbestimmt und willkürgefährdet

Die Formulierung "*Rechtswidrigkeit bereits für einen juristischen Laien ohne weitere Nachforschungen offenkundig*" klingt zwar vernünftig, ist für die Praxis jedoch gefährlich. Rechtswidrigkeiten und im Besonderen Strafbarkeiten (um die es hier ja geht) sind nicht mit dem "gesunden Menschenverstand" beurteilbar, da dieser das moralische Empfinden widerspiegelt, das gerade im Strafrecht oftmals stark von der juristischen Realität abweicht. Die Auslagerung von rechtlichen Entscheidungen an Laien wie hier gefordert führt zu Willkür, was im Sinne einer geordneten Rechtspflege nicht akzeptierbar ist.

getting you ready for tomorrow!
Digital Society | Graben 17/10 | 1010 Wien
ZVR: 547238411 | https://DigiSociety.ngo

§ 4 KoPl-G: Berichtspflicht sehr positiv

Die Berichtspflicht stellt eine wichtige Maßnahme zur Herstellung von Transparenz dar, erst durch Daten über Häufigkeit und Art von Verstößen können rationale Entscheidungen über die Anpassung oder Erweiterung von Maßnahmen gegen den Hass im Netz getroffen werden.

Das es sich hier um ein gesellschaftlich breites Problem handelt, sollte für die genauere Ausgestaltung der Berichte ein entsprechend breiter Konsens durch möglichst vielfältige Einbindung von Stakeholdern geschaffen werden.

Weiters sollte die Vorschreibung einer automatischen Übertragbarkeit der erhobenen Daten erwogen werden. So könnte mit einfachen Mitteln ein konsolidierter Bericht erstellt werden.

§ 5 KoPl-G: Anforderungen an den verantwortlichen Beauftragten sind überschießend, Strafen drakonisch

Von einer einzelnen Person eine persönliche "*jederzeitige Erreichbarkeit*" bei Strafdrohungen bis 10.000€ zu verlangen ist absolut überschießend, um nicht zu sagen unmenschlich. Kein vernünftiger Mensch würde so eine Position annehmen.

Eine solch schwere Verantwortung lässt sich nur gemeinschaftlich tragen, beispielsweise in Form einer juristischen Person.

Positive Effekte der vorgeschlagenen Maßnahmen

Die Initiative gegen Hass im Netz ist sehr zu begrüßen. **Den zivil- und strafrechtlichen Änderungen kann weitgehend zugestimmt** werden, falls die aufgezeigten Probleme behoben werden. Das neue **Kommunikationsplattformen-Gesetz jedoch weist zu viele zu gravierende Probleme auf und sollte daher komplett überarbeitet werden**, da es in der vorliegenden Version nicht die beabsichtigte Wirkung erzielt. Auf Grund der genannten Problematiken erscheit es auch unwahrscheinlich, dass diese innerhalb der aktuell vorgeschlagenen Gesetzesstruktur behoben werden können.

Wir schlagen daher einen anderen Denkansatz für das Kommunikationsplattformen-Gesetz vor:

1. Kommunikationplattformen oberhalb einer bestimmten Anzahl (einer relativ geringen z.B. wenigen tausend) an Nutzer:innen haben ein Beschwerdesystem einzurichten und sind verpflichtet, über die Auslastung desselben Bericht zu

erstatten und diese Daten maschinenlesbar nach einem vorgegebenen Format zur Verfügung zu stellen, sodass diese in eine Übersichtsstatistik einfließen können. Dadurch bleiben triviale Fälle mit stark eingeschränktem und persönlich bekanntem Nutzer:innenkreis wie Plattformen für Familien, Vereine oder innerhalb von Firmen aussen vor, bei denen Hasspostings ein geringeres Problem darstellen, entweder weil sie wegen der persönlichen Bekanntheit kaum auftreten oder weil die Verbreitung gering ist.

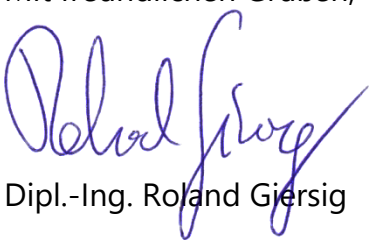
2. Da es nunmehr leichtgewichtige Möglichkeiten gibt, gerichtlich mit Unterlassungsklage auch gegen Plattformbetreiber vorzugehen, siehe § 549 ZPO, sollte es genügen, hier im Rahmen einer Klage die Plattformbetreibenden in die Pflicht zu nehmen und ihnen bei schuldhafter Säumigkeit entsprechenden Schadenersatz für die entstehenden Gerichtskosten zu überantworten. Diese finanzielle Pönalisierung sollte sich primär am erzielten Umsatz orientieren, sodass hier eine automatische Skalierung mit der Größe und kommerziellen Ausrichtung der Plattform gegeben ist.
3. Weiters müssen jedoch auch einem Überblockieren gewisse Schranken gesetzt werden um die Redefreiheit nicht indirekt einzuschränken.

Wir sind uns bewusst, dass dies nur ein sehr grobes Konzept ist, bei dem noch viele Details zu bedenken sind. Dennoch sehen wir hier viele Vorteile durch eine flexible, automatische Regulierung. Sollte ein solches Konzept in Erwägung gezogen werden, so muss es selbstverständlich unter breiter Beteiligung der Stakeholder diskutiert und entwickelt werden, wozu wir gerne einen Beitrag leisten wollen.

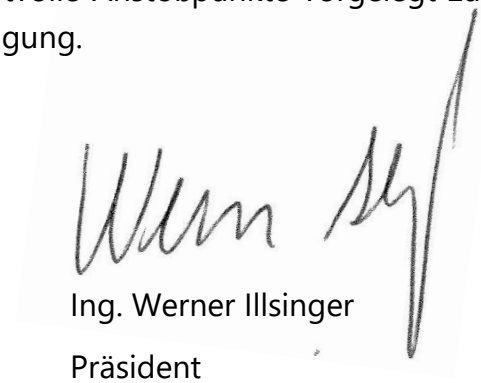
Schluss

Wir hoffen, mit diesen Kommentaren wertvolle Anstoßpunkte vorgelegt zu haben. Für Rückfragen stehen wir gerne zur Verfügung.

Mit freundlichen Grüßen,



Dipl.-Ing. Roland Giersig
Vizepräsident Interessensvertretung
Digital Society



Ing. Werner Illsinger
Präsident
Digital Society

Informationen über uns finden Sie auf unserer Webseite: https://digisociety.ngo/about/
Link zu unseren Stellungnahmen: https://digisociety.ngo/stellungnahmen/

getting you ready for tomorrow!
Digital Society | Graben 17/10 | 1010 Wien
ZVR: 547238411 | https://DigiSociety.ngo