

STELLUNGNAHME ZUM VORENTWURF DES BUNDESGESETZES ÜBER KOMMUNIKATIONSPLATTFORMEN UND SUCHMASCHINEN (KOMPG)

Sehr geehrter Herr Bundesrat Rösti
Sehr geehrte Damen und Herren

Gerne nutzen wir die Möglichkeit, im Rahmen des Vernehmlassungsverfahrens zum Vorentwurf des Bundesgesetzes über Kommunikationsplattformen und Suchmaschinen (KomPG) Stellung zu nehmen.

Der Dachverband Lehrerinnen und Lehrer Schweiz (LCH) äussert sich in dieser Vernehmlassung als die Stimme von rund 55'000 Lehrpersonen auf allen Bildungsstufen der Schweiz. Unsere Legitimation und Dringlichkeit leiten sich direkt aus dem Berufsleitbild und der Berufsethik des LCH ab: Lehrpersonen tragen eine ethische und professionelle Verantwortung für die körperliche und geistige Integrität der ihnen anvertrauten Schülerinnen und Schüler. In den Klassenzimmern erleben Lehrpersonen wiederholt, dass dieser Schutzzanspruch im digitalen Raum derzeit nicht gewährleistet ist. Cybermobbing, Konzentrationsstörungen durch Suchtmechanismen und die Konfrontation mit verstörenden Inhalten gehören für Kinder und Jugendliche zum Alltag. Als Berufsverband sehen wir uns daher in der Pflicht, für das in der Bundesverfassung (Art. 11 BV) und der UN-Kinderrechtskonvention verankerte Recht auf eine gesunde Entwicklung einzutreten.

Der LCH unterstützt das Ziel des KomPG, den digitalen Informationsraum sicherer zu machen und Grundrechte zu stärken (Siehe LCH Positionspapier 'Verantwortungsvoller Umgang mit digitalen Medien (2025)¹). Für einen wirksamen Jugendschutz und den Schutz der Integrität von Kindern und Jugendlichen braucht es jedoch Präzisierungen:

1. **Mindestpflichten sollen für alle in der Schweiz angebotenen relevanten Dienste gelten**, nicht nur für sehr grosse Plattformen.
2. **Schutz von Minderjährigen soll ausdrücklich als eigenständiges Ziel und Querschnittsanforderung im Gesetz verankert werden**.
3. **Melde-, Prüf- und Rückmeldepflichten** müssen bei gravierenden Risiken (z.B. sexualisierte Gewalt, Selbstgefährdung) klarer und verbindlicher geregelt werden.
4. **Empfehlungs- und Werbesysteme** brauchen transparente, nutzerfreundliche Steuerungsmöglichkeiten; profilingbasierte Personalisierung soll mindestens bei Minderjährigen ausgeschlossen werden.
5. **Datenzugang für Aufsicht und Forschung** muss praktikabel ausgestaltet werden (Schnittstellen, Datenkataloge, Schutzvorkehrungen), damit Risiken unabhängig überprüft werden können.
6. **Sanktionen** sollen verhältnismässig, aber wirksam sein und bei systematischen Verstössen auch strukturelle Massnahmen ermöglichen.

Der LCH erachtet das KomPG als wichtigen Baustein, um Grundrechte zu stärken und Verantwortung bei Anbietenden von Kommunikationsplattformen und Suchmaschinen verbindlicher zu verankern. Für einen wirksamen Jugendschutz reicht jedoch Regulierung allein nicht aus. Es braucht eine abgestimmte Gesamtstrategie:

1. **Elternstärkung:** Niederschwellige Beratung und Elternbildung zur Medienerziehung.
2. **Gesetzlicher Schutz:** Verbindliche Massnahmen bei den Diensten selbst, insbesondere Transparenz, sichere Voreinstellungen, wirksame Altersmechanismen sowie Regeln für Empfehlungs- und Werbesysteme.
3. **Schulische Bildung:** Ausbau von Medienbildung und Demokratiekompetenz, begleitet durch ausreichende Ressourcen.

Unsere nachfolgenden Anträge zielen darauf ab, den Vorentwurf so zu präzisieren, dass Schutz und Rechte von Kindern und Jugendlichen im digitalen Raum wirksam und vollzugstauglich umgesetzt werden können.

Freundliche Grüsse

Dagmar Rösler
Zentralpräsidentin LCH

Dr. Beat A. Schwendimann
Leiter Pädagogik LCH

¹ <https://www.lch.ch/publikationen/positionspapiere/detail/verantwortungsvoller-umgang-mit-digitalen-medien>)

ALLGEMEINE BEMERKUNGEN

Der LCH begrüßt das KomPG als Schritt hin zu klareren Pflichten für Kommunikationsplattformen und Suchmaschinen. Dieses schafft endlich einen Rahmen für die Aktivitäten von Kommunikationsplattformen und Suchmaschinen und ihren gesellschaftlichen Auswirkungen. Der Gesetzentwurf sieht wichtige Massnahmen vor, etwa um die Rechte von Nutzerinnen und Nutzer zu stärken und Transparenz zu schaffen über die Funktionsweise der Plattformalgorithmen. Diese Massnahmen sind für eine konstruktive öffentliche Debatte und eine informierte Meinungsbildung von grosser Bedeutung. Aus Sicht der Schule ist aber zudem zentral, dass das Gesetz den Schutz von Minderjährigen und die Stärkung der Grundrechte nicht nur als Absicht formuliert, sondern mit wirksamen, überprüfbaren Instrumenten verbindet.

Ausgangslage aus Sicht der Schule

Kinder und Jugendliche bewegen sich selbstverständlich in digitalen Räumen. Sie sind dabei nicht nur Konsumentinnen und Konsumenten, sondern werden auch gezielt adressiert, beeinflusst und teilweise gefährdet. Befunde aus der JAMES-Studie zeigen, dass sexualisierte Belästigung und unerwünschte sexuelle Anfragen im digitalen Raum verbreitet sind und seit Jahren ein relevantes Problem darstellen: Die Hälfte der Jugendlichen in der Schweiz wurde im Internet schon mit unerwünschten sexuellen Inhalten kontaktiert (Siehe JAMES Studie²). Kommunikationsplattformen werden von Tatpersonen für sexuelle Belästigung, Grooming oder auch das Verbreiten von pädokriminellem Bildmaterial genutzt. Kinder und Jugendliche sehen verstörende Inhalte, sind süchtigmachenden Algorithmen und dark pattern ausgesetzt, sind psychisch belastet wegen Cybermobbing und Hasskommentaren. Es ist dringend notwendig, die Anbieter digitaler Dienste zu Schutzmassnahmen zu verpflichten.

Der LCH unterstützt deshalb die Absicht, der Schweizer Bevölkerung mit der Umsetzung des KomPG mehr Transparenz und Rechte gegenüber Suchmaschinen und Kommunikationsplattformen zu gewähren, bemängelt jedoch die ungenügende Adressierung des Kinder- und Jugendschutzes durch die KomPG Vorlage. Die Vorlage muss neben dem Schutz der Meinungs- und Informationsfreiheit (Art. 16 BV) insbesondere das Recht von Kindern und Jugendlichen auf besonderen Schutz ihrer Unversehrtheit (Art. 11 BV) und das Recht auf körperliche und geistige Unversehrtheit (Art. 10 BV) schützen.

Leitprinzipien für eine wirksame Regulierung

- **Mindestschutz für alle relevanten Dienste:** Kinder und Jugendliche nutzen nicht nur sehr grosse Plattformen. Darum sollen zentrale Mindestpflichten (Meldeweg, Rückmeldung, Schutzvorkehrungen) für alle Dienste gelten, die in der Schweiz angeboten werden und für Minderjährige faktisch zugänglich sind.
- **Risikobasierte Abstufung:** Zusätzliche Pflichten (Audit, systematische Risikoanalyse, erweiterter Datenzugang) sollen abhängig von Reichweite und Risikointensität gelten.
- **Transparenz und Steuerbarkeit:** Nutzerinnen und Nutzer müssen verstehen können, warum ihnen Inhalte oder Werbung angezeigt werden, und einfache, wirksame Einstellungsmöglichkeiten erhalten.
- **Durchsetzung und Nachweisbarkeit:** Pflichten müssen so formuliert sein, dass Aufsicht und unabhängige Forschung deren Wirksamkeit überprüfen können (Datenzugang, Schnittstellen, Reporting).

Der Dachverband Lehrerinnen und Lehrer Schweiz (LCH) fordert deshalb, dass der Gesetzesentwurf erweitert wird, in Ziel und Zweck explizit auch den Schutz von Kindern und Jugendlichen adressiert und Plattformen und Suchmaschinen zu spezifischen Massnahmen verpflichtet. Minderjährige müssen mindestens so gut geschützt werden vor Gefahren im Netz (bspw. digitaler sexualisierter Gewalt, Cybermobbing und Hassrede), wie sie es in der EU bereits sind.

Dazu kommt, dass der Geltungsbereich des Gesetzesvorschlags ungenügend auf die Gefährdungssituation im digitalen Raum eingeht. Kinder und Jugendliche sind nicht nur auf den grossen Kommunikationsplattformen gefährdet, vielmehr ergeben sich Gefährdungen auch auf Online-Game-Plattformen und in Appstores, bezüglich der Verbreitung von pädokriminellem Bild- und Filmmaterial auch bei Hosting- und Cloud-Dienstleistern. In der EU

² <https://www.kinderschutz.ch/uber-uns/medienmitteilungen/james-studie-2022>

sind deshalb mit dem *Digital Services Act* Vorschriften in Kraft, welche unabhängig vom Produkt für die Schaffung eines sicheren digitalen Raumes für Kinder und Jugendliche zentral sind. Ohne entsprechende Regulierung werden diese von den hiesigen Anbietenden nicht freiwillig angewendet. Damit bleiben die Minderjährigen in der Schweiz im digitalen Raum schlechter geschützt als Kinder und Jugendliche in den umliegenden Ländern.

Als weiteren Aspekt weist der LCH darauf hin, dass der Einfluss durch Algorithmen und Künstliche Intelligenz kuratierten Plattformen und Suchmaschinen auf das Wohlergehen von Einzelpersonen sowie auf die demokratische Meinungsbildung weiterhin zunimmt und unser Informationsökosystem sich grundlegend verändert.

Wir sind der Meinung, dass die Schweiz die wichtige Gelegenheit unbedingt nutzen sollte, die der Gesetzesentwurf und der damit angestossene politische Prozess bieten, um diese Herausforderungen zu adressieren und die Verantwortung der Anbietenden sicherzustellen. Entsprechend sind einige Ergänzungen des Gesetzesentwurfes angezeigt. Die drei wichtigsten stellen wir im Folgenden im Überblick vor:

- Ausweitung des Geltungsbereiches auf kleinere, einflussreiche Plattformen prüfen; generative KI-Systeme da erfassen, wo sie als Suchmaschinen oder Social-Media-Plattformen genutzt werden oder in diese integriert sind
- Risikoanalyse ergänzen um die Pflicht, systemische Risiken zu mindern und auch darüber Bericht zu erstatten
- Massnahmen ergänzen, um Selbstbestimmung der Nutzerinnen und Nutzer sicherzustellen und vulnerable Gruppen zu schützen, insbesondere Kinder und Jugendliche

Der aktuelle Vorentwurf zum KomPG ist als Spezialgesetz zu eng gefasst und deckt den tatsächlichen Regelungsbedarf unzureichend ab. Um den verfassungsrechtlichen Schutzauftrag (Art. 11 BV) wirksam zu erfüllen, fordert der LCH stattdessen ein umfassendes Rahmengesetz

Geltungsbereich: Kleinere einflussreiche Plattformen und generative KI

Der aktuelle Vorentwurf beschränkt sich darauf, grosse Plattformen zu regulieren. Diese Fokussierung ist für systemische Risiken nachvollziehbar. Für Jugendschutz und schulrelevante Risiken braucht es jedoch ergänzend Mindestpflichten auch für kleinere, aber in Schulkontexten relevante Angebote (z.B. einzelne Apps, Spiele- und Community-Dienste, spezialisierte Plattformen).

Kleinere, aber unter Umständen ebenfalls einflussreiche Kommunikationsplattformen und Suchmaschinen, die ebenfalls Auswirkungen auf den öffentlichen Diskurs und die Meinungsbildung haben können, bleiben davon ausgenommen. Wichtig ist zu prüfen, ob auch kleinere, Plattformen und Suchmaschinen, die aus anderen Gründen sehr einflussreich sind, einen eingeschränkten Katalog von Mindestpflichten erfüllen sollten (vgl. Stellungnahme zu Art. 2).

Zudem können auch generative KI-Systeme, mit denen sich Texte, Bilder, Audio- oder Videodateien erstellen lassen, bereits heute massive Auswirkungen auf Individuen und die Gesellschaft haben. Etwa, wenn KI-Chatbots für persönliche Beratung in sensitiven Situationen genutzt werden oder wenn mittels generativer KI unzuverlässige oder irreführende Inhalte erstellt werden, die die Meinungsbildung beeinflussen oder Einzelpersonen schaden. Diese Systeme scheinen vom aktuellen Gesetzentwurf, wenn überhaupt, dann nur teilweise erfasst werden zu können. Es ist wichtig, sowohl ein rechtliches Vakuum als auch rechtliche Unsicherheiten bezüglich generativer KI-Systeme zu vermeiden. Es muss klar werden,

- dass grosse KI-basierte Suchmaschinen, KI-Anwendungen, die in grosse Suchmaschinen integriert sind, oder grosse KI-basierte Anwendungen, die als Suchmaschinen genutzt werden, ebenfalls unter das vorgesehene Gesetz fallen,
- dass KI-Anwendungen, die in grosse Social-Media-Plattformen integriert sind, als Teil dieser Plattformen betrachtet werden und somit unter das Gesetz fallen,

- inwiefern weitere generative KI-Anwendungen darunterfallen oder nicht.

Zudem sollten parallel zu dieser Vorlage Massnahmen ergriffen werden, um Anbietenden von generativen KI-Anwendungen, die nicht unter das Gesetz fallen, in die Verantwortung zu nehmen. Es ist dabei entscheidend, dass die Schnittstellen zwischen den künftigen KI-Regulierungen, die der Bundesrat derzeit erarbeiten lässt, und der Plattformregulierung berücksichtigt werden (vgl. Stellungnahme zu Art.2).

Der LCH fordert, dass Dienste der generativen KI dann unter den Geltungsbereich dieses Gesetzes (Art. 2) fallen, wenn sie funktional als Suchmaschinenersatz dienen oder als Kommunikationsplattform für Minderjährige zugänglich sind. Die Definition in Art. 2 ist dahingehend zu präzisieren, dass nicht nur die 'Suche auf Webseiten' (klassische Suchmaschine), sondern auch die 'automatisierte Generierung von Antworten durch generative KI' erfasst wird.

Risikoanalyse und Risikominimierung

Der LCH begrüßt, dass Anbietenden von Plattformen und Suchmaschinen verpflichtet werden sollen, Analysen zu systemischen Risiken durchzuführen. Dies ist eine Kernmassnahme des Gesetzesentwurfs. Wir bedauern jedoch sehr, dass parallel dazu Plattformen und Suchmaschinen nicht verpflichtet werden, auch Massnahmen zu ergreifen, um diese Risiken tatsächlich zu minimieren und über diese Massnahmen zu berichten. Ohne eine solche Risikominderungspflicht müssten die Plattformen zwar Risiken einschätzen aber nichts gegen diese Risiken unternehmen. Damit droht die Regulierung zahnlos zu bleiben (vgl. Stellungnahme zu Art. 20).

Selbstbestimmung und Schutz von Individuen und Gruppen in sensitiven Situationen

Der aktuelle Gesetzentwurf muss die Selbstbestimmung aller Nutzerinnen und Nutzer noch weiter stärken. Es fehlen zudem Bestimmungen zum Schutz von Individuen und Gruppen in sensitiven oder vulnerablen Situationen. Wir sollten die wichtige Gelegenheit, die das geplante Gesetz bietet, nicht verstreichen lassen, um die informationelle Selbstbestimmung sowie den Schutz der Menschen, insbesondere von Kindern und Jugendlichen, zu stärken.

Die Geschäftsmodelle marktmächtiger Plattformen basieren vielfach auf Aufmerksamkeits- und Profitmaximierung, personalisiertem Tracking und algorithmischer Verstärkung. Diese haben Auswirkungen auf die Informationsfreiheit aber auch das Wohlbefinden der Nutzerinnen und Nutzer und insbesondere auf Kinder und Jugendliche. Entsprechend braucht es griffige Massnahmen zur Stärkung der Selbstbestimmung sowie zum Schutz Jugendlicher, wie etwa

- die Aufnahme von negativen Auswirkungen auf Minderjährige in der Liste der systemischen Risiken und die Pflicht, diese Risiken auch zu minimieren (vgl. Stellungnahme zu Art 20),
- eine Einschränkung des Profilings für personalisierte Werbung (u.a. Ausschluss von besonders schützenswerten Personendaten) für alle Nutzerinnen und Nutzer sowie ein Verbot von personalisierter Werbung basierend auf Minderjährigkeit (vgl. Stellungnahme zu Art. 15) und
- die Pflicht, Empfehlungssysteme anzubieten, die nicht auf Profiling und Interaktions- und Aufmerksamkeitsmaximierung basieren (vgl. Stellungnahme zu Art. 18).

Letztlich ist zu betonen: Ein Bundesgesetz zur Regulierung von Social Media und Suchmaschinen kann aber auch in einer ergänzten Form nicht alle Herausforderungen im Zusammenhang mit Plattformen und ihren Auswirkungen auf Mensch und Gesellschaft angehen. Neben der wichtigen Grundlage, die dieses Gesetz bietet, braucht es weitere Schritte und Massnahmen, um der Machtkonzentration grosser Tech-Konzerne zu begegnen und eine konstruktive öffentliche Debatte online zu ermöglichen, die für die Gesellschaft und Demokratie förderlich ist.

Diese Lücke in der Schweizer Gesetzgebung wurde auch im eidgenössischen Parlament erkannt: Entsprechend der Änderung der Mo. Bulliard 24.4020 durch die KVF-S müsste der Jugendschutz im Internet in einem einzigen,

umfassenden Gesetz geregelt werden. Gleichermassen würde der LCH die Stärkung des Jugendschutzes in einem solchen Rahmengesetz für einen sicheren digitalen Raum sehr begrüssen.

FRAGESTELLUNGEN

Das UVEK bittet in der Eröffnung des Vernehmlassungsverfahrens um Stellungnahme zum Meldeverfahren und zu den fehlenden Regelungen zum Kinder- und Jugendschutz. Es formuliert konkrete Fragen. Gerne beantworten wir diese:

1. Wird die Pflicht zur Bereitstellung eines Meldeverfahrens im Grundsatz befürwortet?

Ja, der Dachverband Lehrerinnen und Lehrer Schweiz (LCH) befürwortet die Pflicht zur Bereitstellung eines Meldeverfahren entschieden. Dieses ist ein wichtiger Schritt hin zu einem sichereren digitalen Umfeld. Sie bietet Nutzenden die Möglichkeit, illegale Inhalte niederschwellig zu melden. Für Anbietende bieten solche Meldeverfahren ebenfalls Vorteile: Die Meldungen kommen in gleich strukturierter Form.

Der Meldemechanismus muss unbedingt und ausdrücklich das Ziel verfolgen, Kinder und Jugendliche vor allen Formen von digitaler Gewalt zu schützen. Nur wenn verstörende Gewalt gemeldet wird, kann der Inhalt durch Anbietenden gesperrt oder entfernt werden. Die Meldung von Gewalt muss eine Handlung des Anbietenden auslösen. Der LCH hält zudem die Verpflichtung zur zeitnahen Bearbeitung der Meldungen gemäss Artikel 5 KomPG für essenziell, siehe dazu unseren Kommentar zu Art. 5 VE KomPG weiter unten.

2. Soll das Meldeverfahren auf die in der Vorlage aufgeführten Tatbestände beschränkt bleiben, soll es reduziert oder gestrichen werden oder soll es umgekehrt auf alle rechtswidrigen Inhalte bzw. auf bestimmte rechtswidrige Inhalte ausgeweitet werden?

Der LCH unterstützt die abschliessende Aufzählung unter Artikel 4 des Vorentwurfs zum KomPG nicht. Insbesondere ist für den LCH nicht nachvollziehbar, weshalb der Straftatbestand der verbotenen Pornografie (Art. 197 StGB) sowie andere strafbare Handlungen gegen die physische, psychische oder sexuelle Integrität eines Kindes nicht aufgeführt werden, obwohl diese ihren Ursprung nachweislich oft auf digitalen Kommunikationsplattformen haben. Jeder begründete Verdacht auf eine Straftat gegen die physische, psychische oder sexuelle Integrität eines Kindes soll gemeldet und mit geeigneten Massnahmen wie dem Blockieren der relevanten Inhalte dagegen vorgegangen werden.

Unserer Ansicht nach soll es für sämtliche Arten rechtswidriger Inhalte ein passendes Meldeverfahren geben. Die vorgeschlagene Auflistung von Straftatbeständen ist unvollständig und unflexibel: Bereits jetzt fehlen seit Jahren stattfindende Delikte wie Betrug, Identitätsdiebstahl und Stalking. Zudem wird das Gesetz auch auf zukünftige technische Entwicklungen nicht rasch genug reagieren können. Der LCH befürwortet eine offene Formulierung, damit neue Deliktsformen erfasst werden können.

Aus den genannten Gründen spricht sich der LCH für ein obligatorisches Meldeverfahren für alle mutmasslich rechtswidrigen Inhalte aus – ohne Beschränkung auf einzelne, aufgeführte Tatbestände – analog zu den geltenden Vorgaben des *Digital Services Acts* in der EU. Insbesondere muss das Meldeverfahren unbedingt Anwendung finden auf folgende Straftatbestände:

- Identitätsmissbrauch (Art. 179 decies StGB)
- Sexuelle Handlungen mit Kindern (Art. 187 StGB)
- Verbotene Pornografie (Art. 197 StGB)
- Unbefugtes Weiterleiten von nicht öffentlichen sexuellen Inhalten (Art. 197a StGB)
- Sexuelle Belästigung (Art. 198 StGB)

Die EU und die USA haben dies erkannt und in den jeweiligen Regulierungen von Anbietenden Meldeverfahren und Meldepflichten definiert³. Die schweizerischen Strafverfolgungsbehörden sind hingegen abhängig von ausländischen Meldestellen wie dem amerikanischen NCMEC, um an Informationen über hier verbreitetes und gespeichertes pädokriminelles Material zu gelangen. Bis eine bei NCMEC eingegangene Meldung die zuständige Strafverfolgungsbehörde in der Schweiz erreicht, vergeht viel Zeit, während welcher das Material ungehindert weiterverbreitet wird. Mit einer Ausweitung des Meldeverfahrens im KomPG könnte dieser Weg deutlich verkürzt und die Abhängigkeit von ausländischen Stellen im Kampf gegen Cyberpädokriminalität geschmälert werden. Obwohl einige für den Kinder- und Jugendschutz relevante Delikte wie sexuelle Belästigungen (Art. 198 StGB) explizit genannt sind (Art. 4 Abs. 1 Bst. g KomPG), fordert der LCH, dass gesetzliche Verpflichtungen für Plattformbetreiber auch standardmässige Schutzfunktionen zur Filterung schädlicher Inhalte umfassen müssen, die über die abschliessend aufgeführten rechtswidrigen Tatbestände hinausgehen. Dies ist notwendig, um die Gesundheit, Entwicklung und das Lernen von Kindern und Jugendlichen nicht zu belasten und die verstärkte Bekämpfung von Cybermobbing sicherzustellen.

3. Würden Sie eine Pflicht der geregelten Dienste zur Ergreifung von geeigneten und verhältnismässigen Massnahmen, um für ein hohes Mass an Privatsphäre, Sicherheit und Schutz von Minderjährigen zu sorgen, im Grundsatz begrüssen?

Ja, der LCH erachtet eine Pflicht zur Ergreifung geeigneter und verhältnismässiger Massnahmen zum Schutz von Minderjährigen als dringend notwendig. In der EU sind Anbietenden von Online-Plattformen gestützt auf Artikel 28 des *Digital Services Act* verpflichtet, geeignete und verhältnismässige Massnahmen zu ergreifen, um für ein hohes Mass an Privatsphäre, Sicherheit und Schutz von Minderjährigen zu sorgen. Die Europäische Kommission hat Leitlinien definiert zur Unterstützung von Online-Plattformen bei der Bereitstellung dieser Massnahmen⁴. Der LCH fordert, dass auch die Schweiz die gesetzliche Grundlage schafft für verpflichtende Massnahmen zur Privatsphäre, zum Schutz und zur Sicherheit von Minderjährigen. Die Plattformen müssen verpflichtet werden, Safety-by-design- und Privacy-by-default-Kriterien zum Schutz der minderjährigen Nutzenden konsequent einzusetzen und anzuwenden. Die Notwendigkeit der Entschärfung manipulativer Algorithmen und der Begrenzung riskanter Inhalte durch gesetzliche Massnahmen muss als zentraler Pfeiler im Gesetz verankert werden. Die in Artikel 20 KomPG geforderte jährliche Risikobewertung, welche die negativen Folgen für die Ausübung von Grundrechten der Nutzerinnen und Nutzer erfasst (Art. 20 Abs. 2 Bst. b KomPG), muss explizit die erheblichen Risiken für die Entwicklung und die psychische Gesundheit von Minderjährigen berücksichtigen.

Siehe LCH Positionspapier 'Verantwortungsvoller Umgang mit digitalen Medien (2025):
<https://www.lch.ch/publikationen/positionspapiere/detail/verantwortungsvoller-umgang-mit-digitalen-medien>

Für die konkreten Kriterien siehe die Antwort auf die nächste Frage.

4. Sollten Sie eine solche Pflicht begrüssen, welche der folgenden Massnahmen würden Sie priorisieren?

- a) Bereitstellung eines Meldesystems für Inhalte, die für Minderjährige nicht geeignet sind**
- b) Alterskontrollen**
- c) Bereitstellung eines Systems zur elterlichen Kontrolle**

³ In der EU: [Verordnung \(EU\) 2022/2065 des europäischen Parlaments und des Rates über einen Binnenmarkt für digitale Dienste und zur Änderung der Richtlinie 2000/32/EG](#).

In den USA: [18 U.S. Code § 2258A](#), sowie Präzisierungen im [Report Act \(2024\)](#)

⁴ Mitteilung der Kommission, Leitlinien für Massnahmen zur Gewährleistung eines hohen Masses an Privatsphäre, Sicherheit und Schutz Minderjähriger im Internet gemäss Artikel 28 Absatz 4 der Verordnung (EU) 2022/2065, abrufbar unter: [Mitteilung der Kommission — Leitlinien für Maßnahmen zur Gewährleistung eines hohen Maßes an Privatsphäre, Sicherheit und Schutz von Minderjährigen im Internet gemäß Artikel 28 Absatz 4 der Verordnung \(EU\) 2022/2065](#)

- d) Verbot von Werbung gestützt auf Profiling gemäss Art. 5 Buchstabe f des Datenschutzgesetzes (DSG), wenn hinreichende Gewissheit besteht, dass der betreffende Nutzende minderjährig ist**
- e) Weitere Regelungen zum Kinder- und Jugendschutz**

Der LCH verzichtet auf eine Priorisierung der vorgeschlagenen Schutz-Massnahmen, weil es diese aus unserer Sicht zwingend alle braucht.

Es braucht griffige Massnahmen um den Schutz von Individuen und Gruppen in sensitiven und vulnerablen Situationen, insbesondere von Kindern und Jugendlichen, wie etwa

- die Aufnahme von negativen Auswirkungen auf Minderjährige in der Liste der systemischen Risiken und die Pflicht, diese Risiken auch zu minimieren (vgl. Stellungnahme zu Art. 18)
- die Pflicht, Empfehlungssysteme anzubieten, die nicht auf Profiling und Interaktions- und Aufmerksamkeitsmaximierung basieren (vgl. Stellungnahme zu Art. 18)

Neben diesen Massnahmen, die in den Gesetzentwurf aufgenommen werden können, sind weitere Massnahmen erforderlich, um den Schutz von Kindern und Jugendlichen und anderen Individuen und Gruppen in vulnerablen und sensitiven Situationen zu verstärken, darunter etwa eine Einschränkung von Dark Patterns oder Bildungsmassnahmen (vgl. Begleitmassnahmen).

Nebst Social-Media-Algorithmen beeinflussen zudem auch andere KI-Anwendungen Kinder und Jugendliche, wie beispielsweise KI-Bild- und Videogeneratoren, KI-Chatbots und KI-Gefährten (AI Companions), die zunehmend auch auf Online-Plattformen eingebaut werden. Entsprechend müssen auch die Betreiber von KI-Tools Verantwortung dafür tragen, Massnahmen zu ergreifen, um Nutzerinnen und Nutzer angemessen zu schützen. Wichtig ist entsprechend zu klären, inwiefern solche generativen KI-Anwendungen unter dieses Gesetz fallen oder nicht (vgl. Stellungnahme zu Art. 2).

Um ein sicheres Umfeld für minderjährige Nutzerinnen und Nutzer zu garantieren, braucht es aus Sicht des LCH noch weitere Massnahmen, wie im Folgenden ausgeführt wird.

Zu a): Meldeverfahren allein schützen Kinder nicht ausreichend

Ein Meldeverfahren für ungeeignete, jedoch legale Inhalte ist zwar ein Schritt in die richtige Richtung und grundsätzlich zu begrüßen. Es bietet aber keinen ausreichenden Schutz vor den vielfältigen Risiken, denen Kinder online ausgesetzt sind (z. B. Kontaktaufnahme durch Fremde, Grooming, algorithmische Verstärkung problematischer Inhalte, Exposition gegenüber Gewalt, Radikalisierung oder sexualisierten Inhalten). Um Kinder wirksam zu schützen, braucht es zusätzliche, strukturelle Massnahmen auf Ebene der Plattformen. Anbietenden von Kommunikationsplattformen müssen in proaktive Erkennungs- und Interventionssysteme gegen Cybermobbing und sexuelle Belästigung investieren. Dies korrespondiert mit der Meldepflicht für sexuelle Belästigungen in Artikel 4 Absatz 1 Buchstabe g KomPG und muss eine rasche Reaktion sicherstellen.

Zu b): Altersfeststellung und Altersverifikation sind zentrale Schutzinstrumente

Anbietenden von Kommunikationsplattformen müssen zur **technisch wirksamen, datenschutzkonformen, datensparsamen und verhältnismässigen Altersüberprüfung** verpflichtet werden. Die Leitlinien der Europäischen Kommission geben hierfür geeignete methodische Orientierung. Eine zuverlässige Alterskontrolle ist notwendig, um wirksame und altersgerechte Schutzmassnahmen überhaupt umsetzen zu können. Gesetzlich festgelegte Mindestalter für einzelne Plattformen reichen allein nicht aus, denn sie bieten keinen Schutz vor den tatsächlichen Risiken im Netz. Anbietenden müssen deshalb verpflichtet werden, sichere, altersgerechte Angebote bereitzustellen. Altersbeschränkungen sind dabei als risikomindernde Massnahmen im Rahmen der gesetzlichen Risikoanalyse- und Risikominderungspflichten der Anbietenden zu verstehen.

Zu c): Elternkontrollsysteme sind ergänzend sinnvoll, dürfen aber nicht missbraucht werden

Systeme zur elterlichen Kontrolle können einen nützlichen Zusatzschutz darstellen, dürfen jedoch nicht dazu führen, dass die Verantwortung für den Schutz von Kindern in Bezug auf die Nutzung von

Kommunikationsplattformen auf die Eltern abgewälzt wird. Ebenso dürfen sie nicht in eine unangemessene Überwachung oder Verletzung der Privatsphäre des Kindes münden. Die Hauptverantwortung für den Schutz von Minderjährigen liegt bei den Anbietenden von Kommunikationsplattformen und Suchmaschinen. Sie verfügen über die technischen und organisatorischen Möglichkeiten, den Schutz Minderjähriger wirksam sicherzustellen und müssen entsprechend in die Pflicht genommen werden.

Zu d): Verbot von Werbung auf Profilingbasis schützen Minderjährige

Der LCH unterstützt ein Verbot von Werbung, die auf Profiling von minderjährigen Nutzerinnen und Nutzer basiert. Solche Werbemodelle bergen erhebliche Risiken, da sie Kinder besonders anfällig für Manipulation und problematische Inhalte machen. Zudem begrüßt der LCH die in Artikel 18 Absatz 2 KomPG enthaltene Vorgabe, wonach Anbietenden von Kommunikationsplattformen mindestens eine Option zur Verfügung stellen müssen, deren Empfehlungssysteme nicht auf Profiling gemäss Artikel 5 Buchstabe f DSG beruhen. Dies ist ein wichtiger Schritt, um suchtfördernde Algorithmen und Designelemente zu regulieren oder zu verbieten, manipulative Algorithmen zu entschärfen und zu verhindern, dass Schulen von werbefinanzierten Angeboten abhängig werden.

Zu e) Schweizer Kinder benötigen denselben Schutz wie Kinder in der EU

Kinder und Jugendliche in der Schweiz sollen mindestens denselben Schutz vor Online-Risiken erhalten wie ihre Altersgenossen in der EU. Deshalb müssen die Schutzstandards aus Artikel 28 des Digital Services Act (DSA) auch im schweizerischen KomPG verankert werden. Die gesetzlichen Verpflichtungen sollen Filterung schädlicher Inhalte, die Begrenzung der Nutzungszeit und die Einschränkung riskanter Interaktionen umfassen. Diese Forderungen müssen im Rahmen der Sorgfaltspflichten (Art. 14 KomPG) und der Berücksichtigung der systemischen Risiken (Art. 20 KomPG) konkretisiert werden, um die Gewährleistung der Gesundheit der Kinder zu sichern.

Zusätzlich braucht es die folgenden, konkreten gesetzlichen Verpflichtungen für Plattform-Anbieter:

1. Pflicht zu systematischer Risikoanalyse

Alle Anbietenden – unabhängig von ihrer Grösse – müssen regelmässig eine Risikoanalyse durchführen, die folgende Punkte umfasst:

- Risiken für Privatsphäre, Sicherheit und Schutz Minderjähriger,
- Missbrauchspotenzial der Dienste zur Kontaktaufnahme mit Kindern,
- Risiken der Verbreitung sexualisierter Gewalt oder anderer illegaler Inhalte.

Die Analyse muss auf den Leitlinien der Europäischen Kommission basieren und das Kindeswohl als vorrangigen Gesichtspunkt berücksichtigen.

2. Pflicht zu wirksamen, verhältnismässigen Schutzmassnahmen

Anbietenden müssen die identifizierten Risiken mit nachweislich wirksamen, verhältnismässigen und technologisch aktuellen Massnahmen adressieren. Sie müssen sich bei der Umsetzung dieser Massnahmen zum Jugendschutz an den detaillierten Leitlinien der Europäischen Kommission orientieren. Diese enthalten international anerkannte Standards für Privatsphäre, Sicherheit und Schutz von Minderjährigen.

3. Sanktionen und Präventionsfinanzierung

Die vorgesehenen Sanktionsmöglichkeiten werden begrüßt; sie müssen auch bei unzureichender Umsetzung von Jugendschutzmassnahmen greifen. Zusätzlich sollte ein zweckgebundener Fonds für Prävention digitaler sexualisierter Gewalt geschaffen werden, um das heute bestehende Ungleichgewicht zwischen Milliardengewinnen der Plattformen und fehlender Präventionsfinanzierung auszugleichen.

4. Konsequenter Umgang mit Missbrauch und Hass

Plattformen müssen Nutzerinnen und Nutzer sperren, die Hassrede verbreiten (oder andere Formen von Cybermobbing betreiben) oder andere sexuell belästigen.

5. Sichere Empfehlungssysteme

Plattformen müssen Empfehlungssysteme so gestalten, dass sie Jugendschutzstandards einhalten. Konkret bedeutet dies:

- Keine algorithmische Verstärkung schädlicher Inhalte.

- Kein Hineinführen Minderjähriger in immer extremere Inhalte (bspw. Selbstverletzung, Gewalt, Radikalisierung).
- Klare Begrenzung des unendlichen Scrollens („Endless Scroll“) für Minderjährige.
- Empfehlungssysteme dürfen keine Straftaten gegen Kinder ermöglichen oder erleichtern und nicht zur Verbreitung verbotener Pornografie nach Art. 197 StGB beitragen (Empfehlungssystem = algorithmische Vorschlagsmechanismen wie Feeds, „For You“-Seiten, automatische Videoempfehlungen).

7. Privacy-by-Default und Safety-by-Design

Konten Minderjähriger müssen automatisch mit den höchstmöglichen Datenschutz- und Sicherheitseinstellungen ausgestattet sein. Die Standards sind an Kapitel 6.3 der EU-Leitlinien auszurichten. Zum Safety-by-Design gehört auch, dass KI-Chatbots und KI-Tools für Minderjährige nicht automatisch aktiviert werden. Haben Minderjährige Zugang zu solchen Systemen, müssen diese so konzipiert sein, dass sie dem Entwicklungsstand Minderjähriger entsprechen und keinerlei Risiko für Selbstgefährdung oder suizidales Verhalten darstellen.

STELLUNGNAHME ZU DEN GESETZESARTIKELN

Artikel 1 Zweck

Der LCH schlägt folgende Anpassung vor:

„Dieses Gesetz bezweckt, den digitalen Informationsraum sicherer zu machen, Grundrechte zu stärken und die Transparenz sowie die Rechenschaftspflichten von Kommunikationsplattformen und Suchmaschinen zu erhöhen. Es verpflichtet Anbieter zu wirksamen organisatorischen und technischen Massnahmen zur Prävention und Minderung rechtswidriger und erheblich schädlicher Inhalte. Der besondere Schutz von Minderjährigen ist dabei ausdrücklich zu gewährleisten.“

Artikel 2 Geltungsbereich

Der LCH begrüßt, dass der Geltungsbereich unabhängig ist vom Sitz des Anbieter.

Der LCH fordert zudem, dass die Bedingungen nach Buchstabe a Ziffer 2 ersatzlos gestrichen werden. Der Gesetzentwurf beschränkt sich darauf, nur grosse Social-Media-Plattformen und Suchmaschinen zu regulieren. Kleine Kommunikationsplattformen und Suchmaschinen bleiben unreguliert und generative KI-Systeme, mit denen sich Texte, Bilder, Audio- oder Videodateien erstellen lassen, können, wenn überhaupt, nur teilweise erfasst werden. Mit einer Beschränkung aller gesetzlichen Massnahmen auf Anbieter, die von mindestens 10% der Bevölkerung genutzt werden, fällt die Schweiz hinter die Regulierung derselben im europäischen Kontext zurück. Grundsätzlich wird der digitale Raum für Kinder und Jugendliche nur sicher, wenn alle Plattformen entsprechend reguliert werden.

Als Kommunikationsplattformen gelten auch Dienste mit Kommunikationsfunktionen in Online-Spielen sowie Dienste, die Inhalte Dritter verbreiten oder empfehlen. Der Bundesrat konkretisiert die Abgrenzung so, dass keine Ausweichbewegungen auf nicht erfasste Dienste entstehen.

Vorschlag:

Absatz 1 Dieses Gesetz gilt für Anbieterinnen und Anbieter von Kommunikationsplattformen und Suchmaschinen, die ihre Dienste in der Schweiz anbieten.

Absatz 2 **Mindestpflichten** (insbesondere Meldeweg, Rückmeldung, Schutzvorkehrungen für Minderjährige) gelten für alle Dienste, die für Minderjährige faktisch zugänglich sind.

Absatz 3 **Erweiterte Pflichten** (systematische Risikoanalysen, Audits, erweiterter Datenzugang) gelten für sehr grosse oder besonders risikobehaftete Dienste nach den vom Bundesrat festzulegenden Kriterien.

Verpflichtungen für kleine Plattformen und Suchmaschinen

Grosse Kommunikationsplattformen und Suchmaschinen können mit besonderen systemischen Risiken einhergehen, die besondere Massnahmen rechtfertigen. Gleichzeitig scheint es nicht angebracht, kleinere Dienste automatisch und volumnäßig vom Geltungsbereich der Vorlage auszuschliessen: Insbesondere können Menschen auch auf kleinen Plattformen von Diskriminierung, Hassrede oder anderen schädlichen Inhalten betroffen sein. Ausserdem können auch gesellschaftliche Risiken von kleineren Plattformen ausgehen, da der Einfluss einer Plattform oder einer Suchmaschine nebst ihrer Grösse auch von anderen Faktoren bestimmt werden kann: etwa davon, dass eine besonders hohe Anzahl einflussreicher Persönlichkeiten oder Institutionen dort Informationen austauschen.

Entsprechend sollten auch kleinere, aber aus anderen Gründen einflussreiche Plattformen und Suchmaschinen, die ihre Dienste in der Schweiz anbieten, verpflichtet werden, geeignete Massnahmen zu ergreifen. Diese Plattformen und Suchmaschinen sollten mindestens der Verpflichtung unterliegen einen Transparenzbericht gemäss Art. 19 vorzulegen. Um die Belastung für kleine Unternehmen zu begrenzen, erscheint es sinnvoll, diese Bestimmung auf Plattformen und Suchmaschinen mit mehr als 50 Mitarbeitenden oder einem globalen Umsatz von mehr als 10 Millionen Franken zu beschränken. Zudem ist zu prüfen, ob das in Buchstabe a, Ziffer 2 vorgesehene quantitative Kriterium durch qualitative Kriterien ergänzt werden soll, um festzustellen, ob eine Plattform Risiken birgt, die die Erfüllung weiterer Verpflichtungen erforderlich machen.

Wirtschaftliche Tätigkeit

Die im Gesetzestext gewählte Formulierung «im Rahmen ihrer wirtschaftlichen Tätigkeit» konfiguriert mit Aussagen im Erläuternden Bericht (S. 13 f.), nach welchen gemeinnützigen Plattformen wie Wikipedia nicht vom VE-KomPG erfasst wären.

Das Bundesgericht hat in seiner Rechtsprechung (BGer in Semjud 1994, S. 739 ff.) festgehalten, dass für eine wirtschaftliche Tätigkeit kein Streben nach Gewinn erforderlich ist. Entsprechend reicht das Streben nach Umsatz aus, womit der Wortlaut des Gesetzes Wikipedia miterfasst.

Dieser Widerspruch zwischen Gesetzestext und Erläuterndem Bericht führt zu Rechtsunsicherheit und ist zu vermeiden.

Passung Suchmaschinen

Der LCH begrüßt, dass die Regulierung auch den Bereich der Suchmaschinen umfasst. Suchmaschinen können eine grosse Auswirkung auf die Meinungsbildung haben, denn sie spielen eine entscheidende Rolle für den Informationszugang, die Entscheidungsfindung und die Meinungsbildung von Nutzenden (Nutzende suchen, um Informationen zu erhalten und Entscheidungen zu treffen, und scrollen nicht passiv).

Der LCH sieht jedoch den Bedarf nach Klarstellung, beispielsweise in der Frage, was ein Empfehlungssystem oder die Inhalte-Moderation auf Suchmaschinen genau bedeutet. Aber auch, wie mit den Diensten, die mit Suchergebnissen interagieren und eine Schnittstelle zu ihnen bilden (wie etwa Bewertungen von Dienstleistungen auf Google, die faktisch ein Teil der Suchresultate auf Google sind, aber technisch zum Dienst von Google Maps gehören), umgegangen wird. Zudem ist explizit klarzustellen, dass im Falle von Suchmaschinen, die KI-basierte Suchen in ihre Plattform integrieren (wie etwa der «KI-Modus» oder «AI Overview» im Falle von Google), auch diese Anwendungen als Teil der Suchmaschine betrachtet werden und somit unter das Gesetz fallen. Dieses Beispiel zeigt auch, warum auch für Suchmaschinen Meldeverfahren eine wichtige Stärkung der Nutzenden-Rechte bedeuten würden. Wir würden begrüßen, wenn das Gesetz nach der Vernehmlassung nochmals ganz spezifisch auf die Passung auf Suchmaschinen und die Nutzenden-Rechte überprüft wird.

KI-Chatbots und generative KI

Generative KI-Systeme, mit denen sich Texte, Bilder, Audio- oder Videodateien erstellen lassen, können bereits heute massive Auswirkungen auf Individuen und die Gesellschaft haben. Siehe LCH Positionspapier 'Künstliche Intelligenz': <https://www.lch.ch/publikationen/positionspapiere/detail/kuenstliche-intelligenz-in-der-schule>

Etwa, wenn KI-Chatbots für persönliche Beratung in sensitiven Situationen genutzt werden oder wenn mittels generativer KI unzuverlässige oder irreführende Inhalte erstellt werden, die die Meinungsbildung beeinflussen oder Einzelpersonen schaden. Diese Systeme scheinen vom aktuellen Gesetzentwurf, wenn überhaupt, nur teilweise erfasst werden zu können, nämlich vor allem dann, wenn sie in eine entsprechend grosse Plattform integriert sind oder selbst als eine solche Plattform gelten könnten. Es ist wichtig, sowohl ein rechtliches Vakuum als auch rechtliche Unsicherheiten bezüglich generativer KI-Systeme zu vermeiden.

Entsprechend muss klar werden,

- dass KI-basierte Suchmaschinen, KI-Anwendungen, die in grosse Suchmaschinen integriert sind und KI-basierte Anwendungen, die als Suchmaschinen genutzt werden, ebenfalls ab einer bestimmten Grösse unter das vorgesehene Gesetz fallen. Um diese Klarheit im Falle von Suchmaschinen zu schaffen, könnten Suchmaschinen als Dienste definiert werden, deren Hauptzweck darin besteht, automatisiert und auf Nutzeranfrage hin Informationen zur Verfügung zu stellen.
- dass auch KI-Anwendungen, die in grosse Social-Media-Plattformen integriert sind, dadurch unter das Gesetz fallen. Denn sowohl im Kontext von Suchmaschinen als auch im Kontext von Social Media können generative KI-Anwendungen wesentlich zu systemischen gesellschaftlichen Risiken beitragen, etwa zur massenhaften Verbreitung von sexualisierten Inhalten oder zu unzuverlässiger Information im Kontext von demokratischen Prozessen.
- inwiefern weitere generative KI-Anwendungen darunterfallen oder nicht.

Zudem sollten parallel zu dieser Vorlage Massnahmen ergriffen werden, um Anbietende von generativen KI-Anwendungen, die nicht unter das Gesetz fallen, in die Verantwortung zu nehmen. Es ist dabei entscheidend,

dass die Schnittstellen zwischen den künftigen KI-Regulierungen und der Plattformregulierung berücksichtigt werden.

Artikel 3 (Begriffe)

Art. 3 VE-KomPG definiert einzelne Begriffe, die in der Vorlage vorkommen. Dieser Ansatz ist zu begrüßen. Er schafft Klarheit und damit Rechtssicherheit. Die Definition von Nutzerinnen oder Nutzern weist viele positive Komponenten auf: Er erfasst sowohl natürliche als auch juristische Personen und stellt nicht auf eine Registrierung oder Abonnierung ab.

Der LCH schlägt eine Präzisierung der Begriffe in Art. 3 vor, sodass Online-Vermittlungsdienste für Softwareanwendungen (App Stores) und Online-Gaming-Dienste mit Interaktionsmöglichkeiten explizit als Kommunikationsplattformen gelten, sofern sie Minderjährigen zugänglich sind.

Begründung: Kinder nutzen primär Games beziehen Apps via Stores. Diese Dienste bergen hohe Risiken für Grooming und Kostenfallen. Eine Regulierung, die diese "Gatekeeper" ausklammert, ignoriert die Lebensrealität der Jugend und widerspricht dem Ziel des Jugendschutzes.

Als weitere Präzisierung ist die Definition von 'Nutzung' im VE-KomPG notwendig. Der erläuternde Bericht hält auf S. 15 fest, dass für die Nutzung die Einsicht bei Inhalten genügt. Es erscheint dem LCH dennoch sinnvoll, die Nutzung im Gesetz zu definieren. Mit dieser Ergänzung wird klar, dass es nicht auf die «Einsicht», sondern unter anderem auf den Aufruf, das Teilen oder Herunterladen von Inhalten ankommt. Mit dieser Formulierung werden auch automatisierte Abrufe erfasst, was sonst womöglich nicht der Fall gewesen wäre.

Vorschlag:

In diesem Gesetz bedeuten:

- a. Nutzerin oder Nutzer: natürliche oder juristische Person, die einen Dienst konsumiert oder verwendet, unabhängig davon, ob sie bei dem betreffenden Dienst registriert ist oder diesen abonniert hat;
- b. Empfehlungssystem: vollständig oder teilweise automatisiertes System, das dazu dient, Nutzerinnen und Nutzern Inhalte vorzuschlagen oder diese zu priorisieren.
- c. Der Bundesrat präzisiert Kriterien, die eine organisatorische oder wirtschaftliche Einflussnahme begründen (z.B. Store-Kontrolle, Gatekeeper-Funktionen, Zugangskontrolle, technische Abhängigkeiten).

Artikel 4 Meldeverfahren

Art. 4 sieht für Anbietende von Kommunikationsplattformen und Suchmaschinen die Pflicht vor, ein Meldeverfahren für vermutete Straftaten bereitzustellen. Dies ist aus Sicht des LCH zu begrüßen. Die Auflistung der Tatbestände ist jedoch aus zahlreichen Gründen kein überzeugender Ansatz: Sie ist unvollständig, schwerfällig und führt womöglich zu Fehlanreizen für Anbietende.

Auf den zu regulierenden Diensten finden seit Jahren unzählige Straftaten statt, bei denen die Dienste keine Meldeverfahren einrichten müssten. Darunter sind schwerwiegende Straftatbestände wie Stalking, Identitätsdiebstahl/-missbrauch, Betrug, Erpressung, verbotene Pornografie und Urheberrechtsverletzungen.

Technologische Weiterentwicklungen auf den Plattformen werden auch zur Begehung von potenziell rechtswidrigen Tatbeständen (z.B. Verletzung der Persönlichkeitsrechte, etwa beim Entkleiden von Frauen mit KI-Tools) missbraucht. Eine abschliessende Liste mit Straftatbeständen greift hier zu kurz. Alles, was offline rechtswidrig ist, ist auch online rechtswidrig – und muss gemeldet werden können.

Aus den genannten Gründen sprechen wir uns für ein obligatorisches Meldeverfahren für alle rechtswidrigen Inhalte aus – ohne Beschränkung auf einzelne, aufgeführte Tatbestände.

Vorschläge:

Absatz 1: Ersatz der abschliessenden Aufzählung durch eine offene Norm: «Anbietende stellen ein leicht zugängliches Meldeverfahren bereit, das Meldungen zu rechtswidrigen Inhalten sowie zu erheblich schädlichen Inhalten (insbesondere für Minderjährige) ermöglicht.»

Das Meldeverfahren muss:

- a. niederschwellig, barrierearm und sprachlich verständlich sein,
- b. eine Eingangsbestätigung und eine nachvollziehbare Rückmeldung ermöglichen,
- c. bei Hinweisen auf gravierende Gefährdung (z.B. sexualisierte Gewalt, akute Selbstgefährdung) eine priorisierte Bearbeitung und eine klare Eskalationslogik auslösen.

Die unvollständige Liste sollte gestrichen werden:

~~Es müssen mindestens Inhalte gemeldet werden können, die nach Ansicht der Nutzerinnen und Nutzer einen oder mehrere der folgenden Tatbestände erfüllen:~~

- a. Gewaltdarstellungen (Art. 135 des Strafgesetzbuchs [StGB]);
- b. üble Nachrede (Art. 173 StGB);
- c. Verleumdung (Art. 174 StGB);
- d. Bescämpfung (Art. 177 StGB);
- e. Drohung (Art. 180 StGB);
- f. Nötigung (Art. 181 StGB);
- g. sexuelle Belästigungen (Art. 198 StGB);
- h. öffentliche Aufforderung zu Verbrechen oder zur Gewalttätigkeit (Art. 259 StGB);
- i. Diskriminierung und Aufruf zu Hass (Art. 261bis StGB).

- Explizite Ergänzung der im vorderen Teil genannten Delikte als Mindeststandard, falls eine Liste beibehalten wird: «Mindestens zu erfassen sind Inhalte mit Verdacht auf Straftaten gegen die physische, psychische oder sexuelle Integrität Minderjähriger, namentlich nach Art. 179decies, Art. 187, Art. 197, Art. 197a und Art. 198 StGB.»
- Ergänzung „schädliche, nicht notwendigerweise rechtswidrige Inhalte“ für Minderjährige: «Das Meldeverfahren muss zudem Meldungen zu Inhalten ermöglichen, die Minderjährige erheblich gefährden können, auch wenn sie nicht offensichtlich rechtswidrig sind, insbesondere bei Grooming, sexualisierten Kontakten, Cybermobbing, Hassrede sowie suizid- oder selbstverletzungsbezogenen Inhalten.»

Ergänzend dazu dient die Stellungnahme des LCH zu den Anforderungen an das Meldeverfahren auf Fragen 1 und 2.

Zum Absatz 2:

Der LCH begrüßt, dass anonyme Meldungen möglich sind.

Artikel 5 Bearbeitung der Meldungen und Mitteilungspflicht gegenüber meldenden Nutzerinnen und Nutzern

Art. 5 VE-KomPG sieht keine klar definierten Fristen im Zusammenhang mit der Bearbeitung von Meldungen vor. Das Verwenden der Adjektive «zeitnah» und «unverzüglich» impliziert eine längere Frist bei der Bearbeitung und Entscheidung von Meldungen nach Absatz 1 als bei der Mitteilung über die getroffene Entscheidung nach Absatz 2.

Die Verwendung der beiden undefinierten Rechtsbegriffe führt zu Rechtsunsicherheiten für Anbietende und Nutzende. Gesetzliche Fristen bringen Klarheit für beide Seiten und bedürfen keiner weiteren Auslegung auf Verordnungsebene oder in der Rechtsprechung.

Da die Auflistung der Straftatbestände nach oben erfolgter Argumentation aufgegeben werden soll, ist darüber hinaus eine Anpassung von Absatz 1 notwendig. Entsprechend schlagen wir vor, dass Artikel 5 wie folgt abgeändert wird:

Vorschlag:

Der LCH schlägt dementsprechend folgende Anpassung des Art. 5 vor:

Absatz 1 (neu) Anbietende von Kommunikationsplattformen müssen offensichtlich strafbare Inhalte oder Inhalte, die eine unmittelbare Gefahr für die Integrität von Minderjährigen darstellen, innert 24 Stunden nach Kenntnisserlangung sperren. In komplexen Fällen, die eine vertiefte menschliche Prüfung erfordern,

ist der Zugang zum Inhalt für die Dauer der Prüfung vorsorglich zu sperren, um eine Weiterverbreitung während der Abklärungsphase zu verhindern. Eine definitive Entscheidung erfolgt innert 72 Stunden. Meldende erhalten innert 24 Stunden eine Eingangsbestätigung sowie innert angemessener Frist eine begründete Rückmeldung, sofern deren Meldung die elektronischen Kontaktdaten enthält.

Absatz 2 (neu) Erhalten Anbietende Kenntnis von Inhalten, welche den Verdacht einer Straftat begründen und eine Gefahr für die psychische, physische oder sexuelle Integrität eines Kindes darstellen, so hat sie diesen Verdacht unverzüglich den zuständigen Strafverfolgungsbehörden mitzuteilen und bei der Sicherung, Sperrung und Löschung der Inhalte mit diesen zu kooperieren.

Absatz 3 (neu) Handelt es sich bei den Verdachtsfällen um Inhalte mit pornografischem Inhalt nach Artikel 197 Absätze 4 und 5 des Strafgesetzbuchs, so sind Anbietenden verpflichtet, mit den Strafverfolgungsbehörden oder von Dritten betriebenen Meldestellen zusammenzuarbeiten. Bei Verdacht auf Straftaten gegen die sexuelle Integrität von Kindern sichern die Anbietenden die relevanten Inhalte und Metadaten datenschutzkonform, sperren den Zugriff und melden den Sachverhalt unverzüglich der zuständigen Strafverfolgungsbehörde (Bundespolizei fedpol) nach den gesetzlichen Vorgaben. Die Anbietenden stellen mit angemessenen technischen und organisatorischen Massnahmen sicher, dass gemeldete Inhalte ausschliesslich durch die Strafverfolgungsbehörden oder allenfalls designierten Meldestellen eingesehen werden können.

Absatz 4 (neu) Bei Meldungen zu erheblich schädlichen Inhalten für Minderjährige, die nicht offensichtlich strafbar sind, treffen Anbietenden verhältnismässige Schutzmassnahmen, insbesondere Einschränkung der Auffindbarkeit, der Empfehlung, der Kontaktfunktionen und der Sichtbarkeit für Minderjährige. Sie entscheiden zeitnah und begründen die Massnahme in nachvollziehbarer Form.

Anbietende stellen ein wirksames internes Beschwerdeverfahren für betroffene Nutzerinnen und Nutzer bereit, um Fehlentscheide (z.B. Overblocking) rasch zu korrigieren.

Absatz 5 (neu) Anbietenden nehmen keine eigenständige Sichtung oder Triage mutmasslich pädokrimineller Inhalte vor. Die Sichtung und Triage der gemeldeten Inhalte obliegen den zuständigen Strafverfolgungsbehörden oder allenfalls designierten Meldestellen. Handelt es sich um Verdachtsfälle nach Art. 197 Abs. 4 und 5 StGB, arbeiten die Anbietenden mit Strafverfolgungsbehörden und gegebenenfalls designierten Meldestellen zusammen. Sie stellen mit technischen und organisatorischen Massnahmen sicher, dass gemeldete Inhalte ausschliesslich durch Strafverfolgungsbehörden oder designierte Meldestellen eingesehen werden können.

Absatz 6 (neu) Der Bundesrat erlässt Vorschriften über die sichere technische Übermittlung, Verarbeitung und Dokumentation der Meldungen nach Art. 197 Abs. 4 und 5 StGB. Er regelt die Zusammenarbeit mit inländischen und ausländischen Meldestrukturen. Diese Vorschriften legen zudem die Kooperation der Anbietenden mit privaten Meldestellen, den Strafverfolgungsbehörden und Organisationen im Ausland fest.

Absatz 7 (neu) Der Bund kann mit einer von Dritten betriebenen Meldestelle, zusammenarbeiten. Er gewährleistet die Unabhängigkeit der Meldestelle, soweit sie im Meldeprozess einen Auftrag wahrnimmt. Der Bundesrat regelt die Einzelheiten.⁵

Der LCH fordert zudem, dass Art. 5 VE-KomPG ergänzt wird, indem Anbietenden verpflichtet werden,

- die Konten von Nutzenden zu sperren, die Hassrede verbreiten, sexuelle Belästigung oder andere Verstöße gegen die psychische und sexuelle Integrität von Kindern und Jugendlichen vornehmen;
- mutmasslich strafbare Inhalte innerhalb von 24 Stunden zu sperren;
- Verdachtsfälle, die die Integrität eines Kindes gefährden, unverzüglich den Strafverfolgungsbehörden zu melden;

⁵ Vgl. Art. 46 FMG

- auf Anordnung der Behörden bei der Löschung illegaler Inhalte zu kooperieren;
- bei pädokriminellen Inhalten mit spezialisierten Stellen wie clickandstop.ch zusammenzuarbeiten, um die weltweite Verbreitung zu stoppen;
- das Meldeverfahren auch für illegale Inhalte nach Art. 197 StGB einzurichten;
- keine eigene Triage pädokrimineller Inhalte durchzuführen;

Diese Pflicht gilt auch für Hosting-Provider, auf deren Infrastruktur entsprechende Inhalte gespeichert sind (Integration der Forderung aus Motion 24.4020 Bulliard). *Begründung:* Hosting-Provider müssen in die Pflicht genommen werden, da pädokriminelles Material oft dort lagert und auf Plattformen nur verlinkt wird, selbst wenn diese keine Kommunikationsplattform im engeren Sinne darstellen. Die blosse Löschung von pädokriminellem Material reicht nicht; es muss strafrechtlich verfolgt werden. Die derzeitige Abhängigkeit von US-Meldestellen (NCMEC) verzögert den Schutz der Opfer in der Schweiz massiv.

Bei der Verpflichtung der Anbietenden zur Zusammenarbeit mit Meldestellen sollen erfolgreiche internationale Modelle (z.B. CyberTipline des NCMEC, Stopline Österreich, INHOPE) der Schweiz als Vorbild dienen.

Artikel 6

Der LCH begrüßt, dass der Artikel 6 Transparenz über Moderationsentscheide schafft. Absatz 1 sieht vor, dass Nutzende über einschränkende Massnahmen, von denen sie betroffen sind, informiert werden. Das ist sehr wichtig. Zudem sollten die Plattformen auch verpflichtet sein, diese Entscheide zu begründen.

Vorschlag:

Absatz 1 Ergreifen die Anbietenden einschränkende Massnahmen, begründen sie diese so, dass betroffene Nutzerinnen und Nutzer die Gründe nachvollziehen und ihre Rechte wirksam wahrnehmen können. Die Begründung soll mindestens auf die anwendbare Rechtsgrundlage bzw. Regel, die wesentlichen Tatsachen sowie den verfügbaren Rechtsbehelf hinweisen.

Zudem sollten Nutzende sowohl über einen kompletten Ausschluss von Dienstleistungen als auch über einen teilweisen Ausschluss, etwa wenn die Reichweite ihrer Inhalte beschränkt wird, informiert werden.

Vorschlag:

Absatz 2 [...] c. kompletter oder teilweiser Ausschluss von Nutzerinnen und Nutzern von Dienstleistungen des Anbietenden;

Artikel 7

Es ist erfreulich, dass Art. 7 Absatz 1 vorsieht, dass Beschwerden nicht vollständig automatisiert bearbeitet werden dürfen und eine qualifizierte Person den Prozess beaufsichtigen muss. In der Verordnung zum Gesetz sollte zudem präzisiert werden, dass diese Person über die notwendige Zeit und Kompetenzen, um ihre Aufsichtsaufgaben zu erfüllen, verfügen muss. Es muss ausserdem vermieden werden, dass der Prozess trotz der Anwesenheit eines «Human-in-the-Loop» zu einem «Automation Bias» führt, das heisst zu einer Situation, in der die Person den automatisierten Prozess nicht mehr hinterfragt. Zudem sollte im Absatz 3 «zeitnah» durch eine präzise Zeitangabe ersetzt werden.

Vorschlag:

Absatz 3 Die Anbietende müssen alle Beschwerden innerhalb von 10 Tagen zeitnah bearbeiten und den Nutzerinnen und Nutzern ihre Entscheidung mitteilen.

Teilautomatisierte Moderationsentscheide sind so zu gestalten, dass Fehlanreize und Automatisierungsverzerrungen (Automation Bias) reduziert werden. Nutzende müssen einen wirksamen Zugang zu einer menschlichen Überprüfung erhalten. Der Zeitraum für Beschwerden soll mindestens 30 Tage betragen.

Artikel 8 Zugang und Teilnahme

Der LCH begrüßt die Verfahren zur aussergerichtlichen Streitbeilegung, sie sind ein wichtiges Instrument für die Stärkung der Nutzenden-Rechte. Wir begrüssen es zudem, dass die Verfahren ergänzend (und nicht ausschliessend) sind zu internen Beschwerdeverfahren und ordentlichen Gerichtsverfahren.

Aus Sicht des LCH ist zu klären, dass Nutzenden nicht mit demselben Anliegen gleichzeitig an mehrere Streitbeilegungsstellen gelangen können, da dies zu allenfalls sich widersprechenden Entscheiden führen kann.

Art. 9 Verfahren

Wir schlagen eine Verkürzung beider Fristen auf 60 Tage (statt 90 Tage) vor. Dies ist nutzenden-freundlicher, denn so ist gewährleistet, dass Personen in Kenntnis eines Entscheids der aussergerichtlichen Streitbeilegung überlegen können, ob sie Antragsdelikte (wie beispielsweise die Verleumdung) vor ein ordentliches Gericht bringen wollen. Die Verjährungsfrist bei Antragsdelikten beträgt 3 Monate (ab Kenntnis). Somit würde nur eine verkürzte Frist von 60 Tagen gewährleisten, dass Betroffene nicht in Unkenntnis des Resultats der aussergerichtlichen Streitbeilegung entscheiden müssen, ob sie ein Strafverfahren eröffnen möchten.

Vorschlag:

Absatz 1 Das Verfahren der aussergerichtlichen Streitbeilegung muss binnen 60 90 Kalendertagen nach Eingang der Beschwerde abgeschlossen werden. Bei umfangreichen oder komplexen Fällen kann die aussergerichtliche Streitbeilegungsstelle die Frist nach eigenem Ermessen um maximal 60 90 Kalendertage verlängern.

Artikel 10 Kosten

Die Kosten für die aussergerichtliche Streitbeilegungsstelle sollen hauptsächlich von den Anbietenden der Kommunikationsplattform getragen werden. Diese Kostenverteilung befürwortet der LCH – Nutzende sollen nur in Ausnahmefällen Verfahrenskosten übernehmen müssen. Das entspricht laut dem Erläuternden Bericht (S. 21) auch den gesetzgeberischen Überlegungen.

Statt der Formulierung «böswillig» schlagen wir «missbräuchlich» vor. Damit soll klarer werden, dass die Kostenaufrelegung sich an der Rechtsmissbräuchlichkeit (gemäss Art. 2 Abs. 2 ZGB) orientiert. Wir fordern zudem die Ergänzung des letzten Teilsatzes, so dass die vollen Verfahrenskosten nicht bereits beim ersten Verstoss den Nutzenden auferlegt werden.

Darüber hinaus fordern wir die Deckelung der maximal zulässigen Schutzgebühr auf Verordnungsebene. Damit die Streitbeilegungsstelle eine günstige Alternative zum Rechtsweg bietet, muss die Schutzgebühr maximal 100 Franken betragen.

Vorschlag:

Absatz 1: Die aussergerichtliche Streitbeilegungsstelle kann von der Nutzerin oder vom Nutzer eine Schutzgebühr verlangen. Handelt die Nutzerin oder der Nutzer missbräuchlich böswillig, so kann sie ihr oder ihm die Verfahrenskosten teilweise oder im Wiederholungsfall ganz auferlegen.

Artikel 11 Zulassung

-

Artikel 12 Berichterstattung

-

Artikel 13 Transparenzpflicht

Nutzungsbedingungen sollten für alle Nutzenden, einschliesslich Minderjähriger, verständlich sein. Daher sollten sie adressatengerecht abgefasst werden. Zudem sollten die allgemeinen Geschäftsbedingungen auch in Englisch verfügbar sein.

Vorschlag:

Absatz 3 Die allgemeinen Geschäftsbedingungen müssen in leicht verständlicher Sprache, adressatengerecht, auf Deutsch, Französisch, Italienisch und Englisch abgefasst sein.

Art. 14 Sorgfaltspflicht

Der LCH begrüßt die in Artikel 14 vorgesehene Verpflichtung zur Sorgfalt, Willkürfreiheit und Nichtdiskriminierung sowie die vorgesehenen Massnahmen zur Transparenz der Moderationsentscheide von Plattformen und insbesondere im Absatz 3 die Verpflichtung, die in den Entscheidungsmittelungen verwendeten automatisierten Mittel anzugeben. Eine gute Ergänzung wäre zu informieren, welche automatisierten Mittel zum Einsatz gekommen sind und zu welchem Zweck diese eingesetzt worden sind.

Die Sorgfaltspflicht muss den folgenden Schutzmassnahmen Rechnung tragen:

Vorschlag:

Absatz 1^{bis} (neu):

Anbietende müssen Kinder und Jugendliche durch geeignete organisatorische und technische Massnahmen besonders schützen. Für Minderjährige sind standardmäßig die höchsten Datenschutz- und Sicherheitseinstellungen zu aktivieren (Safety-by-Design). Anbietende sind verpflichtet, ihre Dienste so zu gestalten, dass das Wohl Minderjähriger nicht beeinträchtigt wird (Safety by Design). Dazu gehören: a. Privacy by Default: Voreinstellungen auf höchster Datenschutzstufe. b. Schutz vor Manipulation: Verbot von Designelementen, die zu übermässiger Nutzung oder ungewollten Ausgaben verleiten. c. Datensparsame Altersverifikation: Altersmechanismen sollen risikobasiert, datensparsam und überprüfbar ausgestaltet werden. Die Anbietenden treffen wirksame Massnahmen gegen Grooming, Cybermobbing, Hassrede, sexualisierte Belästigung sowie gegen suchtfördernde Gestaltung.

Absatz 1^{ter} (neu):

Anbietende setzen datenschutzkonforme Systeme zur Altersverifikation ein, die auf dem Prinzip der Datenminimierung beruhen (z.B. Zero-Knowledge-Proofs). Dabei soll insbesondere die Nutzung der staatlichen E-ID (gemäß BGEID) ermöglicht werden, um das Alter zu verifizieren, ohne dass die Plattformbetreiber Zugriff auf die Identitätsdaten der Nutzerinnen und Nutzer erhalten. Die Systeme ermöglichen altersdifferenzierte Schutzmassnahmen, ohne mehr Personendaten offenzulegen als erforderlich.

Absatz 1^{quater} (neu):

Konten Minderjähriger sind standardmäßig mit dem höchstmöglichen Datenschutz und Sicherheitseinstellungen auszustatten. Direkte Kontaktaufnahmen durch unbekannte Erwachsene werden standardmäßig eingeschränkt. KI gestützte Interaktionsfunktionen sind für Minderjährige nicht automatisch aktiviert und müssen dem Entwicklungsstand entsprechen.

Absatz 1^{quinquies} (neu):

Anbietende müssen für Minderjährige standardmässige Schutzfunktionen bereitstellen, insbesondere Filterung schädlicher Inhalte, Begrenzung der Nutzungszeit, Begrenzung riskanter Interaktionen sowie Einschränkung suchtfördernder Mechanismen wie Endlos Scrollen und Autoplay.

Absatz 3:

[...] b. die Angabe, ob automatisierte Mittel zum Einsatz gekommen sind und, wenn ja, welche und zu welchem Zweck

Artikel 15 Werbung

Der LCH begrüßt es sehr, dass sowohl kommerzielle als auch politische Werbung gekennzeichnet werden soll. Für die Informationsfreiheit sollte zusätzlich auch gewährleistet sein, dass Nutzenden Transparenz erhalten über die Auftraggebenden einer Werbung sowie deren Finanzierungsquelle. Dies ist insbesondere im Bereich von politischer Werbung besonders wichtig und würde sich an die Regelung im DSA anlehnen. Wichtig ist auch, dass die Anbietende die Korrektheit der Informationen gewährleisten müssen.

Vorschlag:

Absatz 1 Anbietende von Kommunikationsplattformen oder Suchmaschinen müssen Werbung, die sie gegen Bezahlung oder eine ähnliche Gegenleistung verbreiten, eindeutig als «Werbung» kennzeichnen. Zusätzlich sind Auftraggebende und Finanzierungsquelle transparent auszuweisen. Anbietende müssen angemessene Prüfmechanismen zur Plausibilisierung vorsehen.

Zudem greifen die im Art. 15 vorgeschlagenen Massnahmen nicht weit genug. Aus Sicht des LCH ist eine Ergänzung für ein Verbot von Werbung basierend auf Profiling angezeigt.

Bei Profiling handelt es sich um ein äusserst invasives Geschäftsmodell, mit dem auf Kosten der Privatsphäre und der Integrität der Menschen Werbung verkauft und extremer Reichtum geschaffen wird. Die Nutzenden sind das Produkt, statt selbstbestimmte Akteurin oder selbstbestimmter Akteur im Informationsraum. Mit einem Verbot von durch Profiling personalisierter Werbung verändern wir das Geschäftsmodell hin zu Plattformen und Suchmaschinen, die ihre Dienstleistung ohne derartige Praktiken verkaufen.

Zudem lösen wir damit Probleme, die durch Werbung geschaffen werden, die auf individueller Ebene Wahl- und Abstimmungsverhalten beeinflusst, oder Werbung, welche die Vulnerabilität bestimmter Gruppen (beispielsweise Minderjährige) auszunutzen versucht, oder die auf Personalisierung aufgrund besonders sensibler Persönlichkeitsmerkmale (sexuelle oder religiöse Orientierung, etc.) beruht.

Dass es sich bei personalisierter Werbung, insbesondere wenn sie auf sehr sensiblen Daten beruht, um eine äusserst problematische Praxis handelt, hat jüngst das Urteil des Obersten Gerichtshofs in Österreich im Fall Max Schrems vs. Meta/Facebook vom Dezember 2025 unterstrichen⁶.

Ein Verbot von Werbung basierend auf Profiling heisst nicht, dass Plattformen werbefrei sein müssen. Wie in der analogen Welt und auf diversen Webseiten ist es möglich, allgemeine oder kontextbasierte Werbung zu schalten. Diese ist auf Kontexte zugeschnitten, aber nicht mehr auf einzelne Nutzenden.

Vorschlag:

~~Absatz 2 Sie müssen sicherstellen, dass Nutzerinnen und Nutzer direkt über die Werbung leichten Zugang über die wichtigsten Parameter erhalten können, die bestimmen, welche Werbung ihnen angezeigt wird.~~

(neu): Werbung basierend auf Personendaten der Nutzerinnen und Nutzer (Profiling) ist verboten.

(neu) Netzende müssen direkt bei der Anzeige leicht zugänglich erkennen können, warum ihnen Werbung angezeigt wird (wesentliche Targeting-Parameter).

Absatz 3 (neu): «Anbietenden dürfen keine Werbung auf der Grundlage von Profiling gemäss Artikel 5 Buchstabe f des Datenschutzgesetzes (DSG) unter Verwendung personenbezogener Daten des Nutzers darstellen, wenn sie hinreichende Gewissheit haben, dass die betreffende nutzende Person minderjährig ist.

Begründung: Gerichtliche Entscheide unterstreichen, dass personalisierte Werbung regelmässig einer klaren Rechtsgrundlage und hoher Transparenz bedarf; dies gilt bei Minderjährigen in besonderem Mass.

Artikel 16 Werbearchiv

Der LCH begrüsst, dass ein öffentlich zugängliches Werbearchiv geschaffen werden soll.

Wird Werbung jedoch nur während eines Jahres archiviert, ist es nicht möglich, den öffentlichen Diskurs (Entwicklung von Produkten und Märkten, Meinungsbildung, Kampagnen, soziale Bewegungen) zu analysieren. Nur eine Frist von mehreren Jahren macht Forschung und Analysen praktikabel. Die Frist von 10 Jahren lehnt sich an die übliche Verjährungsfrist für Straftaten (zum Beispiel Art. 261bis StGB mit 10jähriger Verjährung gemäss Art. 97 Abs. 1 lit. c StGB) an, für welche das Werbearchiv relevant sein kann.

Vorschlag:

Absatz 3: Die Werbung muss während der gesamten Dauer ihrer Anzeige auf der Kommunikationsplattform oder Suchmaschine und noch während zehn Jahren eines Jahres nach ihrer letzten Anzeige im Werbearchiv abgefragt werden können.

Parameter, nach denen die Werbung ausgespielt wird und die für Nutzenden transparent sind (gemäss Art. 15), sind ebenfalls im Werbearchiv abzubilden.

⁶ : <https://noyb.eu/de/austrian-supreme-court-meta-must-give-users-full-access-their-data>

Vorschlag:

Absatz 5: Der Bundesrat legt fest, welche Informationen in das Werbearchiv aufgenommen werden müssen. Im Mindesten sind die Parameter abzubilden, welche auch für die Nutzerinnen und Nutzer transparent sind. (gemäss Art. 15)

Um seinem Zweck der Transparenz gegenüber den Nutzenden und der Kontrolle über den Einfluss auf die öffentliche Meinungsbildung nachzukommen, muss das Archiv ohne Hürden zugänglich sein. Nur so ermöglicht es, dass alle Zugriff haben und die notwendigen Analysen durchführen können. Dafür braucht es einen Zugang via API. Auch ein Login auf einer Plattform oder Suchmaschine darf nicht Voraussetzung sein.

Vorschlag:

Absatz 6 neu: Das Werbearchiv ist mittels einer elektronischen Schnittstelle (API) und ohne Registrierungspflicht (Login) zugänglich.

Artikel 17 Kommerzielle Inhalte von Nutzerinnen und Nutzern

Der LCH fordert, dass alle Inhalte mit kommerzieller Absicht – auch Inhalte von Nutzenden – einer Kennzeichnungspflicht unterliegen. Für jugendliche Nutzende kann es schwer sein, die kommerziellen Absichten von Influencerinnen und Influencern zu erkennen. Eine Anzeigepflicht ermöglicht, die kommerzielle Nutzung von Kinderbildern im Netz und die damit einhergehenden Risiken der Ausbeutung des Kindes, der Verletzung des Kindeswohls und der Persönlichkeitsrechte des Kindes zu erkennen. Die Kennzeichnungspflicht gilt in besonderem Mass für Inhalte, die sich an Minderjährige richten oder Minderjährige als Mitwirkende zeigen

Vorschlag:

Absatz 1 Anbietende von Kommunikationsplattformen oder Suchmaschinen müssen den Nutzenden die Möglichkeit anbieten, anzugeben, dass sie den Inhalt zu gewerblichen Zwecken bereitstellen und durch die Bereitstellung des Inhalts den Absatz von Waren oder Dienstleistungen oder das Erscheinungsbild eines Unternehmens fördern wollen.

Absatz 2 Die Anbietende müssen sicherstellen, dass Inhalte nach Abs. 1 markiert werden und der gewerbliche Charakter des Inhalts für andere Nutzerinnen und Nutzer klar erkennbar ist.

Kennzeichnung von Bots

Nutzende haben ein Recht darauf, zu erkennen, ob sie mit einem Konto interagieren, das von Menschen betrieben oder unterhalten wird oder ob es sich um ein Konto handelt, das automatisiert (ohne menschlichen Impuls und Gestaltung) Inhalte postet oder teilt. Die Transparenz darüber ist zentral, um die Informationsfreiheit der Nutzenden zu wahren. Bots können dabei eine durchaus positive Wirkung auf das Informations-Ökosystem haben, beispielsweise indem sie Verkehrsmeldungen automatisiert auf Plattformen spielen. Sie können aber auch ein Faktor sein in der massenhaften Verbreitung von Inhalten, auch von problematischen. Um solche Dynamiken und Meinungsbildungen besser einschätzen zu können, ist es wichtig, dass Bot-Konten transparent sind. Plattformen sollen erstens die Option anbieten, dass bei Einrichtung eines Kontos eine Eigendeklaration stattfinden kann. Sie sollen aber zweitens auch verpflichtet sein, eigene Kenntnis über automatisiertes Posten zu nutzen, um selbst Konten zu kennzeichnen.

Vorschlag:

Zusätzlicher Artikel, der von der Systematik her hier (zwischen Artikel 17 und 18) eingefügt werden soll:

Transparenz über automatisiert Inhalt postende Konten (Bots)

Absatz 1 Anbietende von Kommunikationsplattformen kennzeichnen auf für Nutzerinnen und Nutzer gut sichtbare Weise Konten, welche automatisiert Inhalt posten.

Artikel 18 Empfehlungssysteme

Der LCH begrüßt grundsätzlich, dass mehr Transparenz und Wahlmöglichkeiten zu algorithmischen Empfehlungssystemen geschaffen werden sollen.

Der LCH fordert, dass Anbietenden von Kommunikationsplattformen und Suchmaschinen bei minderjährigen Nutzenden verpflichtet werden, Empfehlungssysteme anzuwenden, welches definierte Parameter zum

Jugendschutz einhält. Des Weiteren sollen die Anbietenden haftbar sein, wenn die Empfehlungssysteme einen Inhalt, der einen Straftatbestand erfüllt, weiterempfehlen.

Zudem sollen alle Parameter transparent gemacht werden; nur so wird das stets vorgeschobene Argument des Geschäftsgeheimnisses obsolet und die nötige Transparenz geschaffen. Es braucht nicht nur eine Information über Möglichkeiten, sondern die Verpflichtung an Plattformen, die Parameter von Algorithmen in Feeds zu ändern und zu personalisieren. Nur so können Nutzende ihre Informationsfreiheit vollständig wahrnehmen. Die Einzelheiten dazu sind vom Bundesrat zu regeln.

Vorschlag:

Absatz 1: Verwenden Anbietende von Kommunikationsplattformen Empfehlungssysteme, so müssen sie:
a. in ihren allgemeinen Geschäftsbedingungen die wesentlichen Parameter, die ihren Empfehlungssystemen zugrunde liegen, sowie deren Gewichtung darlegen;
b. in ihren Einstellungen den Nutzenden die Möglichkeit bieten, die wichtigsten Parameter, die ihren Empfehlungssystemen zugrunde liegen, zu ändern oder zu beeinflussen.
c. (neu) Bei minderjährigen Nutzerinnen und Nutzern wenden Anbietende Empfehlungssysteme mit Jugendschutzparametern an. Empfehlungssysteme dürfen schädliche Inhalte nicht verstärken, nicht in extremere Inhalte führen und keine suchtfördernden Nutzungs dynamiken fördern. Endlos Scrollen und Autoplay sind für Minderjährige standardmäßig zu begrenzen.

Die Verpflichtung, alternative Feeds anzubieten, ist zentral. Diese sollten standardmäßig aktiviert sein, so dass Nutzende aktiv einwilligen müssen, wenn sie ein Empfehlungssystem wählen, das auf Profiling beruht (Opt-in). Wir schlagen vor, die Optionen hier noch zu erweitern und nicht nur Feeds ohne Profiling anzubieten, sondern *zusätzliche* – festgeschrieben durch das Wort «je» – Angebote zu schaffen, die Nutzenden einfach anwählen können. Solche alternativen Feeds sollen die Meinungsbildung in unserer Demokratie durch Informations- und Meinungsvielfalt stärken. Eine weitere Option muss adressieren, dass Nutzenden die Möglichkeit haben wollen, dass nicht Interaktions- und Aufmerksamkeitsmaximierung im Zentrum ihres Informationsökosystems stehen.

Vorschlag:

Absatz 2 (neu):

a. Verwenden Anbietende von Kommunikationsplattformen Empfehlungssysteme, so müssen sie zudem für jedes ihrer Empfehlungssysteme mindestens je eine Option zur Verfügung stellen, die nicht auf Profiling nach Artikel 5 Buchstabe f u. g des Datenschutzgesetzes vom 25. September 2020 (DSG) beruht; die nicht auf Interaktions- und Aufmerksamkeitsmaximierung beruht; die auf die Informations- und Meinungsvielfalt abzielt. Anbietende müssen eine dieser Optionen standardmäßig aktivieren, so dass die Abweichung davon aktiv von den Nutzerinnen und Nutzern angewählt werden muss. Nutzende erhalten wirksame Steuerungsmöglichkeiten (z.B. Deaktivierung profilbasierter Personalisierung, chronologische Darstellung als Option, Begrenzung von sensiblen Themenclustern).
b. Empfehlungssysteme für Minderjährige beruhen standardmäßig nicht auf Profiling. Abweichungen sind nur zulässig, wenn der Anbietende nachweist, dass gleichwertiger Schutz für Minderjährige gewährleistet ist.

Die Transparenz für Nutzende von Suchmaschinen muss ebenfalls erhöht werden. Der Anspruch muss aber nicht derart weitgehend sein wie im Falle von Kommunikationsplattformen, weil die Problemlage bezüglich Meinungsbildung nicht im gleichen Mass akzentuiert ist wie in Feeds auf Plattformen. Sofern mit «Empfehlungssystem» auf Suchmaschinen der Mechanismus der Rangierung von Suchresultaten gemeint ist, würde eine vollständige Transparenz von Sortierparametern zudem das Risiko beinhalten, dass sämtliche Inhalte vollständig auf die Parameter optimiert sind (SEO) – dies würde die Qualität des Rankings negativ beeinträchtigen, bis hin zur Dysfunktionalität. Im Falle von KI-generierten Texten als Suchresultaten (beispielsweise KI-Übersichten auf Google Search) ist die vollständige Transparenz über alle Parameter eine fast unmögliche Aufgabe. Wir schlagen deshalb vor, die Suchmaschinen mit einem zusätzlichen, separaten Absatz und weniger weitgehenden Verpflichtungen zu regeln:

Vorschlag:

Absatz 3 (neu) Verwenden Anbietende von Suchmaschinen Empfehlungssysteme, so müssen sie in ihren allgemeinen Geschäftsbedingungen:

- a. die wichtigsten Parameter, die ihren Empfehlungssystemen zugrunde liegen, sowie deren Gewichtung darlegen;
- b. die Nutzerinnen und Nutzer über allfällige Möglichkeiten informieren, die wichtigsten Parameter, die ihren Empfehlungssystemen zugrunde liegen, zu ändern oder zu beeinflussen.
- c. (Präzisierung Haftungssystematik): Statt einer unklaren Haftungsnorm wird eine Durchsetzung über Sorgfaltspflichten und Sanktionen empfohlen: Verstöße gegen die Jugendschutzparameter gelten als Verletzung der Sorgfaltspflicht und sind verwaltungssanktionsrechtlich zu ahnden. Der Bundesrat regelt Parameter, Prüfanforderungen und Nachweise.
- d. Für Minderjährige sind Schutzvoreinstellungen verbindlich (keine profilbasierte Empfehlung, keine Verstärkung von Inhalten mit hohem Risiko für Gesundheit und Wohlbefinden).

Absatz 4 Verwenden Anbietende von Suchmaschinen Empfehlungssysteme, so müssen sie zudem für jedes ihrer Empfehlungssysteme mindestens je eine Option zur Verfügung stellen, die nicht auf Profiling nach Artikel 5 Buchstabe f des Datenschutzgesetzes vom 25. September 2020 (DSG) beruht.

(neu) Die Wirksamkeit der Massnahmen ist durch Audit- und Aufsichtsinstrumente überprüfbar zu machen (Reporting, Tests, Datenzugang für Aufsicht und qualifizierte Forschung).

Artikel 19 Transparenzbericht

Der in Artikel 19 vorgesehene Transparenzbericht ist eine sehr wichtige Massnahme als Voraussetzung, um Plattformen zur Rechenschaft zu ziehen.

Wichtig ist, dass die Plattformen auch Informationen über die Ergebnisse der Beschwerdeverfahren liefern (unter anderem Erfolgsquote).

Vorschlag:

Absatz 3 c. die Anzahl Fälle, die durch das interne Beschwerdeverfahren nach Artikel 7 und durch eine aussergerichtliche Streitbeilegungsstelle nach den Artikeln 8–12 behandelt wurden und einen Überblick der entsprechenden Ergebnisse.

Um die öffentliche Aufsicht zu erleichtern, sollen alle Berichte vom BAKOM zentralisiert veröffentlicht werden. Zudem soll in der Verordnung festgelegt werden, dass eine Übersicht über die relevante Datengrundlage in einem standardisierten und maschinell lesbaren Format beigelegt werden soll. Dies ist für die Forschung und gesellschaftliche Aufsicht zentral.

Vorschlag:

Absatz 6 Die Anbietende von Kommunikationsplattformen oder Suchmaschinen veröffentlichen den Transparenzbericht in geeigneter Form. Das BAKOM veröffentlicht die Transparenzberichte in einer öffentlich zugänglichen Datenbank in standardisiertem, maschinenlesbarem Format. Es stellt sicher, dass zentrale Kennzahlen vergleichbar sind und zeitnah ausgewertet werden können.

Absatz 7 Die Informationen betreffend die Art und Anzahl der einschränkenden Massnahmen nach Artikel 6 Absatz 2 müssen dem BAKOM ohne Wiedergabe der betroffenen Inhalte übermittelt werden. Das BAKOM veröffentlicht die Informationen in einer Datenbank kann die Informationen in einer Datenbank veröffentlichen.

Artikel 20 Risikobewertung und Risikominimierung

Der LCH begrüßt die Einführung eines Risikobewertungssystems ausdrücklich. Es ist eine Kernmassnahme des Gesetzesentwurfs, dass Anbietende von Kommunikationsplattformen und Suchmaschinen verpflichtet werden sollen, Analysen zu systemischen Risiken durchzuführen.

Es reicht jedoch nicht, wenn die Risikobewertung nur (wie im erläuternden Bericht festgehalten wird) den öffentlichen Diskurs und andere öffentliche Interessen vor tatsächlichen oder möglichen negativen Auswirkungen schützen soll. Es braucht auch eine Risikobewertung bezüglich tatsächlicher oder absehbarer Gefährdung von Minderjährigen.

Zudem fehlt, dass parallel dazu Kommunikationsplattformen und Suchmaschinen verpflichtet werden, auch Massnahmen zu ergreifen, um diese Risiken zu minimieren (es fehlt somit eine Pflicht zu Risikominderung wie sie etwa in Art. 35 DSA vorgesehen ist) und über die getroffenen Massnahmen zu berichten. Ohne solche Verpflichtungen müssten die Plattformen zwar Risiken einschätzen, aber nichts gegen diese Risiken unternehmen. Damit droht die Regulierung zahnlos zu bleiben.

Vorschlag:

Absatz 1 Die Anbietende von Kommunikationsplattformen oder Suchmaschinen müssen jährlich eine Risikobewertung vornehmen, Massnahmen ergreifen, um die identifizierten Risiken zu minimieren, und die Ergebnisse der Bewertung sowie die ergriffenen Risikominimierungsmassnahmen in einem Bericht darlegen. Dieser gibt umfassend Auskunft über die systemischen Risiken in der Schweiz, die durch die Kommunikationsplattformen und Suchmaschinen entstehen oder verstärkt werden, sowie über die Massnahmen, die Anbietende unternehmen, um diese Risiken zu verhindern.

Für Anbietende grosser Dienste gilt zudem, dass sie systematische Risiken identifizieren, bewerten und mindern, insbesondere:

- a. Verbreitung rechtswidriger Inhalte,
- b. negative Auswirkungen auf Grundrechte,
- c. Risiken für die öffentliche Gesundheit und für Minderjährige,
- d. Risiken für das psychische und physische Wohlbefinden (u.a. Suchtmechanismen, Selbstgefährdungsdynamiken),
- e. negative Effekte auf die demokratische Meinungsbildung und den gesellschaftlichen Zusammenhalt.

Definition systemische Risiken

Die Liste der systemischen Risiken im Abs. 2 lit. b muss breiter gefasst und ergänzt werden. Erstens können diese Risiken nicht nur Grundrechte von Nutzenden, sondern auch von Personen betreffen, die die Plattformen selbst nicht nutzen. Zweitens sollten Plattformen auch explizit dazu verpflichtet werden, die systemischen Risiken in Bezug auf geschlechtsspezifische Gewalt, das körperliche und geistige Wohlbefinden einer Person und den Schutz von Minderjährigen zu analysieren, zu mindern und darüber zu berichten.

Vorschlag:

Absatz 2 [...] b. die nachteiligen Auswirkungen auf die Ausübung von Grundrechten der Nutzerinnen und Nutzen, insbesondere in Bezug auf geschlechtsspezifische Gewalt, das körperliche und geistige Wohlbefinden einer Person und den Schutz Minderjähriger und

Absatz 2 Buchstabe b ist wie folgt anzupassen:

«die tatsächlichen oder absehbaren nachteiligen Auswirkungen...»

Drittens sollten im Absatz 2 die durch die Beeinflussung der öffentlichen Debatte und Meinungsbildung entstehenden systemischen Risiken explizit aufgenommen werden. Dabei sollen auch Risiken in Bezug auf das bewusste, massenweise Verbreiten irreführender Informationen (Desinformation) betrachtet werden.

Vorschlag:

Absatz 2 [...]c. Tatsächliche oder absehbare negative Folgen für die öffentliche Meinungsbildung die Beeinflussung der öffentlichen Debatte und Meinungsbildung, von Wahl- und Abstimmungsprozessen, sowie negative Folgen für die öffentliche Sicherheit und Ordnung sowie und die öffentliche Gesundheit.

Der LCH fordert zudem folgende Ergänzungen:

Vorschlag:

Absatz 2 Buchstabe d (neu):⁷

«tatsächliche oder absehbare nachteilige Auswirkungen in Bezug auf den Schutz von Minderjährigen, geschlechtsspezifische Gewalt, Grooming, Cybermobbing und Hassrede sowie schwerwiegende negative Folgen für das körperliche und geistige Wohlbefinden einer Person.»

⁷ Analog zu Absatz 34 Abs 1 Bst d DSG

Absatz 3 (Präzisierung):

Die Risikobewertung erfasst auch Risiken durch Empfehlungssysteme, Profiling, manipulative Gestaltung und Interaktionsfunktionen, soweit sie Minderjährige betreffen.

Form, Verfahren und Veröffentlichung

In der Verordnung soll festgelegt werden, dass eine Übersicht über die relevante Datengrundlage in einem standardisierten und maschinell lesbaren Format beigelegt werden muss. Dies ist für die Forschung und gesellschaftliche Aufsicht zentral.

Zudem ist für die gesellschaftliche Aufsicht wichtig, dass das BAKOM standardmäßig die Berichte veröffentlicht (vgl. Stellungnahme zu Art. 37).

Vorschlag:

Absatz 4 Die Anbietende müssen dem BAKOM den Bericht über die Ergebnisse der Risikobewertung und Risikominimierungsmassnahmen gemeinsam mit dem Evaluationsbericht nach Artikel 25 übermitteln und ihn veröffentlichen. Das BAKOM veröffentlicht die wesentlichen Ergebnisse in geeigneter Form und kann zusätzliche Auflagen verfügen, wenn Massnahmen nicht wirksam sind.

Absatz 6 (neu)

Anbietenden ergreifen angemessene und wirksame Risikominderungsmassnahmen, die auf die ermittelten Risiken zugeschnitten sind. Dazu gehören Massnahmen zum Schutz vor ungeeigneten Inhalten, zur Sicherheit und zum Datenschutz durch Technikgestaltung, zur Begrenzung riskanter Interaktionen sowie zur proaktiven Erkennung und Intervention bei Cybermobbing, Grooming und sexueller Belästigung. Der Bundesrat regelt die Einzelheiten. Der Bund regelt die Einzelheiten.⁸

Artikel 21 Bezeichnung und Zugang

Die Meldestelle ist eine sinnvolle Ergänzung der Rechte der Nutzenden. Wir schlagen zwei Ergänzungen vor: Nutzende sollen sie auch auf Englisch kontaktieren können – dies ist wichtig, da Englisch einerseits eine landesweiter Schulsprache ist und andererseits in der Schweiz zahlreiche Menschen leben, die zugezogen und keiner Amtssprache mächtig sind. Zudem soll eine Antwort innerhalb von 24 Stunden erfolgen. Dies ist wichtig, um wirklich einen guten Service in der schnelllebigen Online-Welt zu bieten. Viele Anliegen vertragen nicht den Aufschub von mehreren Tagen.

Vorschlag:

1 Die Anbietende von Kommunikationsplattformen oder Suchmaschinen müssen eine Anlaufstelle bezeichnen, über die die Nutzerinnen und Nutzer und das BAKOM sie rasch auf elektronischem Weg in einer Amtssprache oder auf Englisch erreichen können und innerhalb von 24 Stunden eine Antwort erhalten.

Artikel 22 Kommunikation

Die Ergänzung von Art. 22 Abs. 2 stellt sicher, dass Nutzende bei relevanten Anliegen nicht ausschliesslich auf automatisierte Systeme angewiesen sind. Gerade bei komplexen Sachverhalten, bei Eingriffen in Nutzendenrechte oder bei strittigen Entscheidungen stossen automatisierte Verfahren an ihre Grenzen. Der garantierte Zugang zu einer menschlichen Ansprechperson stärkt den Rechtsschutz, erhöht die Nachvollziehbarkeit von Entscheidungen und trägt dazu bei, Fehlentscheide sowie Missbrauch oder Diskriminierung durch automatisierte Systeme zu vermeiden.

Vorschlag:

Absatz 2 Die Anbietende von Kommunikationsplattformen oder Suchmaschinen müssen sicherstellen, dass den Nutzerinnen und Nutzern neben automatisierten Mitteln stets auch eine menschliche Ansprechperson zur Verfügung steht. Die Nutzerinnen und Nutzer haben das Recht, eine automatisierte

⁸ Siehe dazu bspw. Leitlinien der europäischen Kommission zum Schutz durch Technikgestaltung. Der Vorschlag zu Abs. 6 ist dem Art. 35 des Digital Services Act der EU angelehnt.

Kommunikation auf eine menschliche Bearbeitung zu übertragen dürfen nicht ausschliesslich automatisierte Mittel einsetzen.

Artikel 23 Bezeichnung

Das Zustellungsdomizil ist ein etablierter Rechtsbegriff im schweizerischen Prozessrecht im Gegensatz zur Rechtsvertretung. Es ist deshalb zentral, diese beiden Begriffe miteinander zu verbinden. Die Erweiterung ist wichtig, weil die Erläuterungen des VE-KomPG (Ziffer 4.2.10) die Rechtsvertretung nur als Zustelldomizil gemäss Art. 11b Abs. 1 VwVG beschreiben. Im Verwaltungsrecht erfolgt eine Beschränkung der Rechtsvertretung bzw. des Zustellungsdomizils auf Verwaltungsbehörden. Bezüglich des vorliegenden Gesetzes wäre dies konkret das BAKOM. Die Ergänzung erweitert das Zustelldomizil auch auf Anliegen anderer Behörden wie Strafbehörden oder Zivilgerichte (durch den ausdrücklichen Bezug auf Straf- und Zivilrecht).

Nur wenn allen Behörden ein Zustelldomizil zur Verfügung steht, sind die Motionen 18.3306 und 18.3379 zur stärkeren Rechtsdurchsetzung, welche das Parlament bereits 2018 und 2019 mit grosser Mehrheit überwies, vollständig erfüllt.

Vorschlag:

Absatz 1 Anbietende von Kommunikationsplattformen oder Suchmaschinen, die nicht in der Schweiz niedergelassen sind, müssen eine juristische oder natürliche Person in der Schweiz als ihre Rechtsvertreterin oder ihren Rechtsvertreter bezeichnen. Die bezeichnete Rechtsvertretung ist gleichzeitig das Zustellungsdomizil im Sinn von Art. 140 ZPO, Art. 87 StPO und Art. 11b VwVG.

Artikel 24 Unabhängige Evaluation

Der LCH begrüßt die Pflicht zur unabhängigen Evaluation der Umsetzung gesetzlicher Vorschriften. Die vorgesehene externe Evaluation ist ein sinnvolles Instrument. Damit eine externe Evaluation jedoch den gesetzlich festgelegten Zielen gerecht wird, muss die Unabhängigkeit der Dienstleister, die diese Evaluationen durchführen, gewährleistet sein. Es ist wichtig, dass hierfür ausreichende Kriterien festgelegt werden. Entscheidend ist zudem, dass die Evaluationsorganisationen auch erwiesenermassen über das erforderliche fachliche Know-how verfügen.

Artikel 25 Evaluations- und Massnahmenbericht

Der LCH begrüßt die Regelungen zum Evaluations- und Massnahmenbericht. Es ist jedoch für die gesellschaftliche Aufsicht wichtig, dass das BAKOM standardmäßig die Berichte veröffentlicht (vgl. Stellungnahme zu Art. 37).

Vorschlag:

Absatz 3 Innert drei Monaten nach Erhalt des Evaluationsberichts müssen die Anbietende den Evaluationsbericht ohne Personendaten sowie, wenn Mängel festgestellt sind, den Massnahmenbericht über die ergriffenen Massnahmen ohne Personendaten veröffentlichen und dem BAKOM übermitteln. Das BAKOM veröffentlicht die Berichte ebenfalls ~~Das BAKOM kann die Berichte ebenfalls veröffentlichen.~~

Art. 26 Datenzugang für Forschungsorgane und zivilgesellschaftliche Organisationen

Stand heute ist Forschung zu den Auswirkungen von Online-Plattformen auf Einzelpersonen und die Gesellschaft nur erschwert möglich beziehungsweise bleibt punktuell oder experimentell, da die Plattformen kaum verlässlichen Zugang zu den relevanten Daten ermöglichen. Während diese privaten Plattformen unsere öffentliche Debatte kuratieren und beeinflussen, bleibt Forschung im öffentlichen Interesse dazu also weitgehend unmöglich.

Um eine verlässliche und systematische Faktenbasis über die gesellschaftlichen Auswirkungen von Social Media und Suchmaschinen zu erlangen, benötigen wir jedoch genau solche Forschung. Der im Vorentwurf vorgesehene Artikel 26 schafft eine essenzielle Grundlage dafür und ist ein wesentlicher Bestandteil der Rechenschaftsstruktur der vorgesehenen Regulierung, insbesondere in Kombination mit anderen Rechenschaftsmassnahmen wie der Risikoanalyse (Art. 20) und der unabhängigen Evaluationen (Art. 24). Artikel 26 ergänzt diese Pflichten auf wichtige Weise, da er es externer Forschung ermöglicht, die Ergebnisse dieser Analysen zu bestätigen, ergänzen und/oder davon abweichen zu können. Wir begrüssen somit die Regelung in Artikel 26 ausdrücklich, insbesondere die im Absatz 4 definierte Rolle und Entscheidungskompetenzen des BAKOM als Vermittlerin zwischen Forschenden und Plattformen. Gleichzeitig schlagen wir wenige Präzisierungen und Ergänzungen vor.

Vorschlag:

Anbietende stellen für qualifizierte Forschung und Aufsicht einen praktikablen Datenzugang bereit, der Risiken im digitalen Raum unabhängig überprüfbar macht. Dazu gehören:

- a. Datenkataloge (Metadaten, Definitionen, Aktualisierung, Dokumentation),
- b. Schnittstellen für öffentlich zugängliche Daten (API oder gleichwertige Lösung),
- c. klare Schutzvorkehrungen (Datensicherheit, Vertraulichkeit, Datenschutz, Minimierung).

Die Regelung soll sich an anerkannten Standards zum Datenzugang orientieren, wie sie im europäischen Kontext für sehr grosse Dienste entwickelt wurden.

Zugangsberechtigte

Wir begrüssen ausdrücklich die Möglichkeit für zivilgesellschaftliche Organisationen, die nachweisen können, dass sie im öffentlichen Interesse recherchieren, keine kommerziellen Interessen verfolgen und einen angemessenen Datenschutz gewährleisten können, Zugang zu Daten zu bekommen. Solche Organisationen haben in der Vergangenheit eine wichtige Rolle dabei gespielt, Plattformen zur Rechenschaft zu ziehen und haben im Rahmen ihrer unabhängigen und gemeinwohlorientierten gesellschaftlichen Aufsichtsfunktion die öffentlich zugänglichen Daten der Plattformen auf beeindruckende Weise genutzt. Wir plädieren ausdrücklich dafür, diese Antragsberechtigung für zivilgesellschaftliche Organisationen beizubehalten.

Wir gehen zudem davon aus, dass auch Konsortien aus Zugangsberechtigten, die mit weiteren zivilgesellschaftlichen Organisationen, Journalistinnen und Journalisten sowie unabhängigen Forscherinnen und Forscher zusammenarbeiten, Zugang zu den Daten erhalten können.

Datenzugang erleichtern

Absatz 2 sieht vor, dass die Daten, zu denen Zugang beantragt wird, im Antrag bezeichnet werden sollen. Dies kann jedoch für Forschende schwierig sein, weil die Plattformen keinen Überblick über die Daten geben, über die sie verfügen. Eine Möglichkeit, um dies zu lösen wäre, dass Plattformen Datenkataloge veröffentlichen, wie es auch der DSA vorsieht. Die derzeit verfügbaren Kataloge haben sich aber bisher als unbrauchbar erwiesen. Eine andere Möglichkeit wäre, die Datenbezeichnung im Antrag möglichst breit zu lassen, und Plattformen zur Zusammenarbeit mit Forschenden zu verpflichten, um die Anforderungen der Forschung zu erfüllen.

Transparentes Verfahren und Widerspruchsmöglichkeit

Wir begrüssen die im Absatz 4 definierte Rolle und Entscheidungskompetenzen des BAKOM als Vermittlerin zwischen Forschenden und Plattformen. Das Verfahren zur Genehmigung von Zugangsanträgen muss transparent sein und Forschenden ermöglichen, Widerspruch einzulegen.

Vorschlag:

Absatz 4 Das BAKOM übermittelt die bewilligten Anträge an die jeweiligen Anbietende und verpflichtet sie, innerhalb einer angemessenen Frist Zugang zu den entsprechenden Daten zu gewähren. Wird ein Antrag abgelehnt, begründet das BAKOM dies, und die Antragsteller haben die Möglichkeit, Widerspruch einzulegen.

Zugang zu öffentlichen Daten

Zudem sollten Plattformen Schnittstellen bereitstellen müssen, um verlässlichen Zugriff auf öffentlich zugängliche Daten für Forschung im öffentlichen Interesse zu gewähren (vgl. Art. 40.12 DSA). Dies würde es Forschenden ermöglichen, nach bestimmten Themen oder Inhalten zu suchen, Inhalte nach der Aktivität der Nutzenden zu ordnen oder zu sehen, welche Konten bestimmte Narrative verbreiten. Anbietende sind bereits durch den DSA dazu verpflichtet. Entsprechend wäre dies für sie keine zusätzliche Belastung.

Weiter muss sichergestellt werden, dass Online-Plattformen unabhängige, legale und datenschutzkonforme Forschung mittels anderer Methoden (etwa mittels Datenspenden oder Scraping) nicht verhindern, indem sie Forschende unter Druck setzen, ihre Zugänge willkürlich entziehen oder ihnen Einschüchterungsklagen androhen.

Vorschlag:

Absatz 4 (neu) Anbietende gewähren Zugang zu öffentlich zugänglichen Daten in einer Online-Suchschnittstelle, einschliesslich, soweit technisch möglich, zu Echtzeitdaten. Organe und Organisationen, die die Bedingungen im Absatz 1 erfüllen, können den Zugang zur Schnittstelle erhalten.

Absatz 5 Anbietende dürfen unabhängige, legale und datenschutzkonforme Forschung mittels anderer Methoden (etwa mittels Datenspenden oder Scraping) nicht verhindern.

Art. 27 Aufsicht

Der LCH begrüßt, dass das BAKOM mit den Aufsichtskompetenzen beauftragt wird. Dies ist angesichts der bisherigen Aufgaben und Kompetenzen der Behörde sinnvoll. Um seine Aufsichtstätigkeiten erfolgreich ausüben zu können, muss das BAKOM jedoch verlässlich über die notwendigen Ressourcen und Kapazitäten sowie die erforderliche Expertise verfügen. Dies scheint mit den aktuell geplanten fünf bis zehn zusätzlichen Vollzeitäquivalenten (gemäss RFA) nicht gewährleistet zu sein.

Zudem kann eine Aufsichtsbehörde alleine die facettenreichen gesellschaftlichen Auswirkungen und systemischen Risiken nicht alleine beurteilen. Es braucht ein konstruktives Ökosystem von Forschenden, Zivilgesellschaft und Behörden, um dies zu ermöglichen und Forschung an systemischen Risiken voranzutreiben. Außerdem ist ein iteratives Vorgehen und ein «Dual-Track»-Ansatz, wie ihn AlgorithmWatch bezüglich dem DSA vorschlägt hier angezeigt⁹. Dieser ermöglicht es dem BAKOM, mit Unterstützung durch Expertinnen und Experten sicherzustellen, dass eine breite und vielfältige Palette von Datentypen zugänglich ist, jedoch durch einen klaren und nachvollziehbaren Prozess. Vor diesem Hintergrund schlagen wir auch vor, die Aufsichtsbehörde von einem Beirat aus Zivilgesellschaft, Wirtschaft, Wissenschaft und unabhängigen Organisationen begleiten zu lassen (vgl. DSC-Beirat in Deutschland), um externe Aufsicht und Expertise einfließen zu lassen.

Weiter sollte die Regulierung kombiniert werden mit einem unabhängigen, interdisziplinären Kompetenzzentrum auf nationaler Ebene – einem «Digital Media Observatory» für die Schweiz. Dieses soll Expertinnen und Experten aus Wissenschaft, Zivilgesellschaft, Bildung und Medien zusammenbringen, um die Forschung in diesem Bereich voranzutreiben.

Art. 28 Auskunftspflicht

Anbietende sollen dem BAKOM innert angemessener Frist Auskunft geben. Diese Handhabung macht Sinn, da sie dem BAKOM Flexibilität gibt und die Frist somit der Komplexität der Anfrage angepasst werden kann. Dennoch erachten wir es als sinnvoll, eine gesetzliche Vermutung für den Zeitaufwand einer Auskunftserteilung vorzugeben. Damit wird den Anbietenden ein Richtwert vorgegeben, an dem sie sich orientieren können. Gleichzeitig kann bei besonders dringlichen oder besonders aufwändigen Auskunftsersuchen von dieser Frist abgewichen werden.

Vorschlag:

Absatz 1 Die Anbietende von Kommunikationsplattformen oder Suchmaschinen müssen dem BAKOM innert angemessener Frist Auskunft erteilen und ihm sämtliche Daten im Sinne von Artikel 38 herausgeben, die zur Wahrnehmung seiner Aufsichts- und Evaluationsaufgaben erforderlich sind.

Absatz 2 Der Auskunftspflicht unterliegen auch Rechtsvertreterinnen oder Rechtsvertreter von Anbietende von Kommunikationsplattformen oder Suchmaschinen.

Absatz 3 Die Auskunft wird in der Regel innerhalb von 30 Tagen erteilt.

Art. 29 Beaufsichtigte Unternehmen

Art. 30 Gebühren

Art. 31 Aufsichtsaufgabe

Der LCH begrüßt den vorgeschlagenen Ansatz mit zweistufiger Finanzierung.

Artikel 32 Verwaltungsmassnahmen

Abs. 2 entspricht sogenannten Netzsperren: Der Zugang zu einem ganzen Dienst (eine Website in ihrem Ganzen) wird gesperrt.

⁹ (<https://algorithmwatch.org/en/dual-track/> und <https://algorithmwatch.org/en/researching-systemic-risks-under-the-digital-services-act/>)

Klärungsbedarf in Bezug auf Netzperren

Eine solche Massnahme schränkt die Grundrechte (hier die Meinungs- und Versammlungsfreiheit) von potenziell sehr vielen Nutzenden ein und geht entsprechend mit hohen Anforderungen an deren Rechtfertigung einher, da die Verhältnismässigkeit der Massnahme gegeben sein muss. Es muss somit sichergestellt sein, dass die Massnahme geeignet, zumutbar und erforderlich ist, um das Ziel zu erreichen. Aus diesem Grund wäre eine solche Befugnis auch nur im Sinne einer *ultima ratio* anzuwenden. Diese Qualifizierung fehlt derzeit im Gesetzestext und wäre gegebenenfalls zu ergänzen. Zudem ist sicherzustellen, dass eine solche Massnahme auch tatsächlich geeignet ist, um das Ziel zu erreichen. Aufgrund der grenzüberschreitenden Natur der Plattformen stellen sich zudem praktische Hürden bei der Durchsetzbarkeit einer solchen Massnahme, da Nutzenden andere Wege finden können, um die Plattform weiterhin zu nutzen.

Vorschlag:

- Absatz 1 Stellt das BAKOM eine Rechtsverletzung nach diesem Gesetz fest, so kann es von der für die Verletzung verantwortlichen juristischen oder natürlichen Person verlangen:
- a. die Verletzung zu beheben und Massnahmen zu ergreifen, damit die Verletzung sich nicht wiederholt;
 - b. das BAKOM über die ergriffenen Massnahmen zu unterrichten.

Absatz 2 Erweisen sich die Massnahmen als unwirksam oder besteht Grund zur Annahme, dass sie unwirksam sind, so kann das BAKOM die Fernmeldedienst-Anbietende anweisen, den Zugang zu einer Kommunikationsplattform oder Suchmaschine einzuschränken.

Artikel 33 Verfahren bei Einschränkung des Zugangs zum Dienst

Falls Netzperren eingesetzt werden sollten, so ist es zwingend nötig, dass nicht eine Amtsbehörde alleine eine solche Massnahme aussprechen kann. Dies eröffnet der politisch-administrativen Willkür Tür und Tor. Ein derart weitgehender Eingriff ist mindestens mit einer richterlichen Entscheidung abzusichern, welche sicherstellt, dass eine Interessenabwägung zwischen verschiedenen Rechtsgütern stattfindet. Die Dauer einer Netzperre ist entsprechend festzulegen.

Zudem sind verfahrensrechtliche Schutzvorkehrungen wie auch Rechtsmittelmöglichkeiten für betroffene Nutzenden vorzusehen.

Aus Sicht des LCH ist der Schutz von Kindern und Jugendlichen vor systemischer Gewalt höher zu gewichten als die wirtschaftlichen Interessen von Plattformbetreibern, die sich einer Regulierung verweigern. Eine starre Obergrenze von 30 Tagen für Zugangsbeschränkungen ist daher abzulehnen, wenn die Gefahr fortbesteht.

Vorschlag:

Absatz 2:

Das BAKOM soll die Möglichkeit haben, den Zugriff als *ultima ratio* so lange einzuschränken, bis die festgestellte schwerwiegende Rechtsverletzung behoben ist. Um die Verhältnismässigkeit und die Informationsfreiheit zu wahren, ist bei Massnahmen, die länger als 30 Tage dauern, eine richterliche Bestätigung vorzusehen. Die Sperrung muss sich technisch so gezielt wie möglich auf die rechtswidrigen Bereiche des Dienstes beschränken.

(Präzisierung): Die Einschränkung dauert an, bis die festgestellte Rechtsverletzung behoben ist und organisatorische und technische Massnahmen eine Wiederholung verhindern.

Artikel 34 Sanktionen

Der LCH begrüßt die griffigen Sanktionsmöglichkeiten, die im Artikel 34 vorgesehen sind. Diese sind zentral für eine wirksame Rechtsdurchsetzung. Insbesondere begrüssen wir, dass diese Sanktionen vor dem Hintergrund der enormen Umsätze der grossen Plattformunternehmen festgelegt werden, damit diese tatsächlich eine abschreckende Wirkung entfalten können.

Der LCH unterstützt einen wirksamen, abgestuften Sanktionskatalog. Sanktionen sollen sich nach Schwere, Systematik und Kooperationsbereitschaft richten. Bei wiederholten oder systematischen Verstößen sind neben Bussen auch strukturelle Massnahmen (z.B. befristete Einschränkungen einzelner Funktionen) vorzusehen.

Der Katalog ist so zu formulieren, dass Vollzug und gerichtliche Überprüfung möglich bleiben (klare Tatbestände, Nachweisbarkeit, Verhältnismässigkeit).

Es ist erfreulich, dass der Vorentwurf die Berechnungsgrundlage für Sanktionen und den maximalen Prozentsatz aus dem europäischen Recht übernimmt. So wird ein Beitrag geleistet zur internationalen Kohärenz. Ebenfalls zu begrüssen ist, dass diese parallel zu Verwaltungsmassnahmen nach Artikel 32 angewendet werden können.

Der LCH lehnt jedoch die in den Absätzen 1 und 2 vorgeschlagene Unterscheidung zwischen Verletzungsart und entsprechenden Sanktionsmöglichkeiten ab. Diese beiden Absätze weisen dem BAKOM ein Ermessen zu bei der Strafzumessung. Es wird nur die Maximalhöhe vorgegeben, entsprechend braucht es diese Differenzierung nicht. Zudem soll die Pflicht, angemessene Massnahmen zu ergreifen, um systemische Risiken zu mindern und darüber Bericht zu erstatten, im Katalog ergänzt werden.

Weiter ist die Verantwortlichkeit von Organen bis hin zu sonstigen natürlichen Personen der Normalfall im Schweizer Recht, wenn Sanktionen verhängt werden. So zum Beispiel auch im neuen Datenschutzgesetz (Art. 60 ff DSG), wo es sich als sehr wirksam erwiesen hat, oder als Grundsatz im Strafgesetzbuch (Art. 102 StGB). Es liegt auf der Hand, dies auch im KomPG umzusetzen: Um die Durchsetzung des KomPG zu stärken ist es nötig, die verantwortlichen Organe der Plattformen und Suchmaschinen bis hin zu den Entscheidungsträgerinnen und -träger in die Pflicht zu nehmen den Verpflichtungen nachzukommen. Das BAKOM behält den in Abs. 5 (bzw. bisher Abs. 4) zugestandenen Ermessensspielraum auch in der Zuschreibung von Verantwortung an Organe oder Personen.

Vorschlag:

Der LCH ergänzt, dass Verstösse gegen Jugendschutzpflichten explizit sanktionsfähig sein müssen.

Absatz 1 (neu):

«Das BAKOM eröffnet von Amtes wegen oder auf Anzeige hin ein Verfahren, wenn Anhaltspunkte für eine Rechtsverletzung nach diesem Gesetz bestehen.»

Der LCH fordert folgende Ergänzungen:

Absatz 1 Buchstabe h (neu):

«gegen die Pflicht verstösst, festgestellte systemische Risiken mit der Umsetzung angemessener Massnahmen zu mindern.»

Zusätzlich Absatz 1 Buchstabe. i (neu):

«gegen Pflichten zum Schutz Minderjähriger nach Art. 4, Art. 5, Art. 14, Art. 15 Abs. 3, Art. 18 und Art. 20 verstösst.»

Absatz 2 (bisher Abs. 1)

Das BAKOM kann einem Anbietenden einer Kommunikationsplattform oder Suchmaschine mit einem Betrag von bis zu 6 Prozent des in den letzten drei Geschäftsjahren durchschnittlich weltweit erzielten Jahresumsatzes belasten, wenn diese:

- a. gegen eine rechtskräftige Verfügung des BAKOM verstösst;
- b. gegen die Pflicht zur Einrichtung eines Meldeverfahrens (Art. 4) oder eines Verfahrens zur Bearbeitung von Meldungen (Art. 5) verstösst;
- c. gegen die Pflicht zur Einrichtung eines internen Beschwerdeverfahrens verstösst (Art. 7);
- d. es systematisch ablehnt, an einer aussergerichtlichen Streitbeilegung teilzunehmen (Art. 8);
- e. gegen die Bestimmungen über die transparente Kennzeichnung von Werbung (Art. 15) oder die Pflicht zur Einrichtung eines Werearchivs (Art. 16) verstösst;
- f. gegen die Pflicht verstösst, eine Funktion anzubieten, mit der Nutzerinnen und Nutzer angeben können, ob der von ihnen bereitgestellte Inhalt kommerzielle Absichten verfolgt (Art. 17);
- g. gegen die Pflichten betreffend Empfehlungssysteme (Art. 18) verstösst
- h. gegen die Transparenzpflicht betreffend allgemeine Geschäftsbedingungen (Art. 13) verstösst;
- i. gegen die Sorgfaltspflichten (Art. 14) verstösst;
- j. gegen die Bestimmungen über den Transparenzbericht (Art. 19) und den Bericht über die Ergebnisse der Risikobewertung (Art. 20) verstösst;

- k. keine Anlaufstelle bezeichnet, die diesbezüglichen Informationen nicht aktuell hält oder sie nicht leicht zugänglich macht (Art. 21 und 22);
- l. keine Rechtsvertreterin oder keinen Rechtsvertreter bezeichnet, die diesbezüglichen Informationen nicht aktuell hält oder sie nicht leicht zugänglich macht (Art. 23);
- m. gegen die Bestimmungen über die unabhängige Evaluation (Art. 24 und 25) verstößt;
- n. Forschungsorganen und zivilgesellschaftlichen Organisationen den Zugang zu Daten unberechtigterweise nicht gewährt oder verweigert (Art. 26);
- o. gegen die Auskunftspflicht (Art. 28 Abs. 1 und Art. 29) verstößt oder
- p. neu «gegen die Pflicht verstößt, systemische Risiken mit der Umsetzung angemessener Massnahmen zu mindern und darüber Bericht zu erstatten.» (Art. 20).

(bisheriger Abs. 2 aufgelöst, da keine Differenzierung der maximalen Bussenhöhe mehr)

Absatz 3 (neu): Das BAKOM kann natürliche Personen, die als Organe, Mitglieder eines Organs, Mitglieder der Geschäftsleitung oder als faktisch verantwortliche Personen eines Anbietenden tätig sind, mit einem Betrag von bis zu 250 000 Franken belasten, wenn sie vorsätzlich oder fahrlässig dieses Gesetz im Sinn von Art. 34 Abs. 2 verletzen oder solche Verletzungen anordnen, fördern oder nicht verhindern, obwohl sie dazu verpflichtet gewesen wären.

Absatz 4 (neu) Der Bund errichtet einen zweckgebundenen Fonds. Dieser wird primär durch die Einnahmen aus Verwaltungssanktionen nach Artikel 34 gespeist. Reichen diese Mittel nicht aus, leistet der Bund ergänzende Beiträge. Die Fondsmittel werden insbesondere verwendet für den Betrieb unabhängiger Meldestellen, für nationale Präventions- und Aufklärungskampagnen sowie zur Unterstützung interkantonaler Koordinationsaufgaben im Bereich der Medienbildung. Zudem können Projekte kofinanziert werden, welche Schulen und Lehrpersonen bei der Förderung der Medienkompetenz entlasten, namentlich durch die Bereitstellung von offenen Bildungsmaterialien (Open Educational Resources) oder nationalen Plattformen. Der Bundesrat regelt die Einzelheiten.

Artikel 35: Verjährung

Die im VE-KomPG enthaltenen Verjährungsfristen entsprechen den Verjährungsfristen aus dem Verwaltungsstrafrechtsgesetz (Art. 11 VStrR). Wie oben ausgeführt, überzeugt die Kategorisierung der Verwaltungssanktionen in 2 Stufen nicht. Mit Anpassung von Art. 34 VE-KomPG wird auch die Aufteilung der Verjährungsfrist nach Verletzungstatbestand hinfällig. Wir fordern stattdessen eine Vereinheitlichung der Verjährungsfrist für sämtliche Verletzungen des VE-KomPG. Sie soll einheitlich 7 Jahre betragen.

Vorschlag:

Absatz 1 Die Befugnis zur Verhängung von Sanktionen verjährt bei Verletzungen des Gesetzes nach Artikel 34 Absatz 1 nach sieben Jahren und bei allen anderen Verletzungen nach vier Jahren.

Artikel 36 Grundsatz

-

Artikel 37 Information der Öffentlichkeit

Die Verfügungen sowie die von den Plattformen erhaltenen Berichte (vgl. Art. 9 und Art. 20) sollten öffentlich zugänglich sein. Die in Absatz 3 vorgesehenen Bestimmungen könnten die Möglichkeiten der öffentlichen Kontrolle und die Fähigkeit der Gesellschaft, Risiken zu bewerten und Plattformen zur Verantwortung zu ziehen, erheblich beeinträchtigen. Es muss klar festgehalten werden, wann der Schutz von Berufs-, Geschäfts- oder Fabrikationsgeheimnissen angebracht werden darf. Dabei muss sichergestellt werden, dass dieser nicht bezüglich Daten von öffentlichem Interesse angebracht werden darf.

Vorschlag:

Absatz 1 Das BAKOM informiert die Öffentlichkeit regelmässig und verständlich über Risiken, Trends und Vollzugserfahrungen (z.B. häufige Deliktskategorien, Wirksamkeit von Massnahmen, Beschwerde- und Bearbeitungszeiten). Veröffentlichungen erfolgen so, dass Schutzinteressen von Minderjährigen und Datenschutz gewahrt bleiben.

Absatz 2 Es veröffentlicht seine Verfügungen und macht sie online zugänglich kann seine Verfügungen veröffentlichen und sie online zugänglich machen.

Absatz 3 Es gibt keine Berufs-, Geschäfts- oder Fabrikationsgeheimnisse preis. Es berücksichtigt dabei gerechtfertigte Berufs-, Geschäfts- oder Fabrikationsgeheimnisse auf angemessene Weise, wenn diese nicht dem Zweck des vorliegenden Gesetzes zuwiderlaufen oder missbräuchlich vorgebracht werden, um den Bestimmungen gemäss Kapitel 2 dieses Gesetzes nicht Folge zu leisten.

Ergänzender Handlungsbedarf ausserhalb des KomPG

Der LCH weist darauf hin, dass Jugendschutz im digitalen Raum nur im Zusammenspiel mit Prävention, Bildung und Unterstützung gelingt. Dazu gehören insbesondere der Ausbau von Medienbildung und Demokratiekompetenz sowie ausreichend Ressourcen für Schulen und Lehrpersonen.

Art. 38 Bearbeitung von Daten juristischer Personen und Personendaten

-

Art. 39 Internationale Zusammenarbeit und Vereinbarungen

-

Art. 40 Evaluation

-

Begleitmassnahmen

Das Bundesgesetz über Kommunikationsplattformen und Suchmaschinen allein wird nicht ausreichen, um alle Herausforderungen im Zusammenhang mit Plattformen und ihren Auswirkungen auf Einzelpersonen und die Gesellschaft anzugehen. Weitere Massnahmen sind notwendig, um der Machtkonzentration grosser Tech-Konzerne zu begegnen und eine konstruktive öffentliche Debatte zu ermöglichen, die für die Gesellschaft und Demokratie förderlich ist. Folgende weiteren Massnahmen sollten in Verbindung mit und parallel zu dem Gesetz vorgesehen werden.

Massnahmen zur Marktmacht

Die Unternehmen hinter Online-Plattformen üben nicht nur eine enorme Meinungsmacht, sondern gleichzeitig auch eine grosse Marktmacht aus. Auch aus ökonomischer Sicht sind solche Machtkonzentrationen nicht nachhaltig. Entsprechend sollte eine Plattformregulierung ergänzt werden mit entsprechenden Massnahmen, um auch der Marktmacht der Plattformunternehmen zu begegnen. Ein effektives Kartellrecht im digitalen Bereich setzt dabei eine kontinuierliche Beobachtung der regulatorischen Entwicklungen in der Europäischen Union, ex-ante Regulierungen (wie etwa im Digital Markets Act der EU vorgesehen), eine ausreichend ausgestattete und handlungsfähige Wettbewerbskommission (WEKO) sowie eine enge internationale Zusammenarbeit und Koordination mit ausländischen Wettbewerbsbehörden voraus. Es ist zudem sicherzustellen, dass auch grosse Technologiekonzerne mittels einer Sorgfaltspflicht Verantwortung für ökonomische, soziale und ökologische Aspekte in ihren Wertschöpfungsketten übernehmen.

Demokratieförderliche Alternativen für den Zugang zu verlässlicher Information entwickeln

Wir brauchen gemeinwohlorientierte Alternativen zu der Dominanz weniger globaler Plattformen, die ihren Profit durch verhaltensbasiertes Profiling und möglichst lange Nutzungsdauer maximieren und damit die informierte Meinungsbildung beeinträchtigen. Dies ist wichtig, um sowohl den Grundrechtsschutz der Bevölkerung als auch die staatliche Handlungsfähigkeit, die «Digitale Souveränität», zu gewährleisten.

Entsprechend sollten algorithmische Empfehlungssysteme, Plattformdesigns oder auch alternative Plattformen entwickelt und gefördert werden, die demokratieförderlich sind, die also den Zugang zu verlässlicher Information und zu vielfältigen journalistischen Inhalten sicherstellen und eine konstruktive Debattenräume ermöglichen. Dazu sollten auch digitale Güter und Infrastrukturen im öffentlichen Interesse bereitgestellt werden. Der Zugang zu Online-Debattenräumen und zu verlässlichen, vielfältigen Informationen muss dabei für alle Menschen gewährleistet sein. Siehe LCH Positionspapier 'Politische Bildung (2024)'¹⁰

Förderung digitaler Souveränität im Bildungswesen

Eine Regulierung kommerzieller Plattformen reicht nicht aus. Der Staat muss sicherstellen, dass die obligatorische Schule ihre Aufgaben erfüllen kann, ohne Schülerinnen und Schüler in die Abhängigkeit datensammelnder Grosskonzerne zu treiben. Der Bund soll gemeinsam mit den Kantonen den Aufbau und Betrieb von datenschutzkonformen, werbefreien Open-Source-Infrastrukturen für den Bildungsbereich fördern, die als sichere Alternativen zu kommerziellen Plattformen dienen.

Erweiterung Art. 261bis StGB

Menschen müssen sich wirksam und niederschwellig wehren können gegen illegale Inhalte, die Menschen diskriminieren, die zu Hass, Hetze und Gewalt an einer bestimmten Gruppe aufstacheln oder Darstellungen von sexualisierter und anderer Arten von Gewalt zeigen. Dies bedingt, dass Betroffene einfach straf- und zivilrechtliche Mittel ergreifen können gegen jene, die den entsprechenden Inhalt erstellt und online gestellt haben. Dafür sollte unter anderem das Strafgesetzbuch in Art. 261bis StGB um den Schutz vor Diskriminierung aufgrund der Geschlechtsidentität erweitert werden, da beispielsweise Frauen sehr oft von Hassrede betroffen sind.

Dark Patterns und Addictive Designs einschränken

Manipulativ gestaltete Benutzungsoberflächen («Dark Patterns») und Addictive Designs haben negative Auswirkungen auf Nutzenden. Unhendliche Timelines verleiten Nutzende zu maximaler Nutzungsdauer und damit Interaktion mit Inhalten. Die Verwendung von Dark Patterns ist allerdings nicht nur bei

¹⁰ <https://www.lch.ch/publikationen/positionspapiere/detail/politische-bildung-in-der-schule-staerken>

Kommunikationsplattformen ein Problem für Nutzende. Auch abseits davon, zum Beispiel im Bereich Online-Shopping und bei Apps, werden Dark Patterns verwendet, um Nutzende gezielt zu manipulieren. Es ist wichtig, dass auch die Schweiz wirksame Regulierungsansätze zur Bekämpfung von schädlichen Dark Patterns verfolgt. Dabei ist auch zu prüfen wie Dark Patterns, die die Nutzungsdauer maximieren sollen, beschränkt werden können. Siehe LCH Positionspapier 'Verantwortungsvoller Umgang mit digitalen Medien (2025)'¹¹

Medien-, Digital- und Demokratiekompetenz fördern

Die Förderung von Medien- und Digitalkompetenzen sind für alle Altersgruppen, durch verschiedene Kanäle und zielgruppengerechte Formate, zu stärken. Dabei geht es einerseits um die Vermittlung von Kompetenzen, um die Funktionsweise der Online-Plattformen, ihrer Algorithmen und deren Auswirkungen zu verstehen. Andererseits beinhaltet dies auch Massnahmen im Bereich der politischen Bildung, der gesellschaftlichen Bedeutung einer inklusiven, konstruktiven Debatte oder der Demokratiekompetenz, um kritische Reflexion im Umgang mit Technologie und informierte demokratische Meinungsbildung zu befördern. Für diese Massnahmen sind die entsprechenden Ressourcen durch die öffentliche Hand bereitzustellen. Siehe Positionspapier LCH:

Interdisziplinäre Forschung fördern

Unabhängige und interdisziplinäre Forschung zu den Funktionsweisen von Plattformalgorithmen sowie insbesondere zu ihren Auswirkungen auf Mensch und Gesellschaft muss gefördert und finanziert werden. Die dadurch gewonnene Evidenzbasis würde die Gesellschaft in ihrem Umgang mit Plattformen und die Aufsichtsbehörden bei der Umsetzung des Gesetzes unterstützen. Die Resultate dieser Forschung sind öffentlich zugänglich zu machen. Weiter sollte die Regulierung mit einem unabhängigen, interdisziplinären Kompetenzzentrum auf nationaler Ebene – einem «Digital Media Observatory» für die Schweiz kombiniert werden. Dieses soll Expertinnen und Experten aus Wissenschaft, Zivilgesellschaft, Bildung und Medien zusammenbringen, um die Forschung in diesem Bereich voranzutreiben

Journalismus und Medien fördern

Für demokratische Gesellschaften sind eine gemeinsame Faktenbasis und informierte Meinungsbildung zentral. Um sicherzustellen, dass die Bevölkerung Zugang zu qualitativ hochwertigen, vielfältigen und verlässlichen Informationen hat, spielen die Medien eine zentrale Rolle. Eine vielfältige, starke Medienlandschaft und qualitativ hochstehender Journalismus sind in der Schweiz deshalb durch umfassende und zeitgemäße Förderungsmassnahmen sicherzustellen.

Schnittstellen mit der KI-Regulierung klären

Derzeit laufen mehrere Arbeiten zur Regulierung von Algorithmen und KI. Es ist wichtig, die Kohärenz zwischen diesen Regelungen zu gewährleisten – insbesondere vor dem Hintergrund, dass oft dieselben Anbietende hinter Plattformen und KI-Systemen stehen. Deshalb sollte die Plattformregulierung als ein Puzzleteil der Regulierungen rund um KI betrachtet werden.

Der LCH dankt Ihnen für die Möglichkeit zur Stellungnahme und die Berücksichtigung unserer Anmerkungen.

¹¹ <https://www.lch.ch/publikationen/positionspapiere/detail/verantwortungsvoller-umgang-mit-digitalen-medien>