RheinlandPfalz
MINISTERIUM DER JUSTIZ

- per E-Mail an: Geschäftsstelle@landtag.rlp.de -

Ministerium der Justiz Rheinland-Pfalz| Postfach 32 60 | 55022 Mainz

Präsident des Landtags Rheinland-Pfalz
Herrn
Hendrik Hering, MdL
Platz der Mainzer Republik 1
55116 Mainz

LANDTAG
Rheinland-Pfalz
18/2019
VORLAGE

DER MINISTER

Ernst-Ludwig-Straße 3
55116 Mainz
Zentrale Kommunikation:
Telefon 06131 16-0
Telefax 06131 16-4887
Poststelle@jm.rlp.de
www.jm.rlp.de

07. Juni 2022

Mein Aktenzeichen	**Ihr Schreiben vom**	**Ansprechpartner/-in / E-Mail**	**Telefon / Fax**
4009E22-0063			06131 16-4856
Bitte immer angeben!		Ministerbuero@jm.rlp.de	06131 16-4844

Sitzung des Rechtsausschusses des Landtags Rheinland-Pfalz am 3. Juni 2022
TOP 7: „Entwurf der EU-Kommission zur sogenannten Chat-Kontrolle“

Antrag der Fraktion der FDP nach § 76 Abs. 2 GOLT
– Vorlage 18/1957 –

Sehr geehrter Herr Präsident,

in der vorbezeichneten Sitzung hat der Rechtsausschuss die Landesregierung zu TOP 7 um Übersendung des Sprechvermerks gebeten. Dieser Bitte komme ich gerne nach und übersende Ihnen den für die Sitzung vorbereiteten Text des Sprechvermerks:

> *„Am 11. Mai 2022 hat die EU-Kommission den Entwurf einer Verordnung zur Verhinderung und Bekämpfung des sexuellen Missbrauchs von Kindern vorgestellt. Bisher liegt dieser Entwurf nur in englischer Sprache vor.*
>
> *Ein wesentlicher Inhalt dieser Verordnung sind Vorgaben für Anbieter interpersoneller Kommunikationsdienste und Hosting-Dienste im Internet.*

Unter den Begriff der interpersonellen Kommunikationsdienste fallen alle Dienste, die eine Kommunikation zwischen Menschen ermöglichen, also etwa Chat- aber auch E-Maildienste. Zu den Hosting-Diensten zählen beispielsweise die Veröffentlichung von Webseiten oder das Bereitstellen von Dateispeicher im Netz.

Diese Dienstleister sollen dazu verpflichtet werden, das im Rahmen der Nutzung ihrer Dienste bestehende Risiko des sexuellen Missbrauchs von Kindern anhand vorgegebener Kriterien zu bewerten und erforderlichenfalls Maßnahmen zu ergreifen, um diesem Risiko entgegenzuwirken. Den Bericht über diese Risikobewertung müssen sie an die zuständige staatliche Stelle übersenden, die den Prozess begleitet und überprüft.

Kommt die staatliche Stelle zu dem Ergebnis, dass entsprechende präventive Maßnahmen ausgeschöpft wurden und dennoch ein erhebliches Risiko eines Kindesmissbrauchs bei Nutzung dieses Dienstes verbleibt, so kann sie eine richterliche „detection order“ - auf Deutsch etwa einen „Erkennungsbeschluss“ - beantragen.

Damit kann sie den Dienstleister verpflichten, die über seinen Dienst erfolgende gesamte Kommunikation für einen bestimmten Zeitraum systematisch zu durchsuchen und zwar nach bekanntem oder neuem kinderpornographischen Bildmaterial sowie nach Hinweisen auf „Grooming“. Unter „Grooming“ versteht man die virtuelle Kontaktaufnahme mit einem Kind mit dem Ziel, es sexuell zu missbrauchen.

Der Diensteanbieter soll zu diesem Zweck eine Software einsetzen, die von einer neu einzurichtenden europäischen Behörde namens „EU-Zentrum“ zur Verfügung gestellt wird. Er kann aber auch eine eigene Software einsetzen, wenn diese bestimmten Anforderungen genügt.

Setzt ein Dienstleister eine solche Überwachungs-Software ein, muss er seine Kunden hierüber grundsätzlich in Kenntnis setzen und über mögliche Rechtsbehelfe informieren.

Meldet die eingesetzte Software einen Treffer, d.h. ein potentiell kinderpornographisches Bild oder einen Hinweis auf Grooming, muss der Dienstleister für jeden Treffer einen Bericht an das neue EU-Zentrum übermitteln.

Dort wird der Treffer überprüft. Fehlerhafte Berichte - also solche, aus denen sich offenkundig keine Hinweise auf eine einschlägige Straftat ergeben - werden aussortiert. Die übrigen Berichte werden an Europol und – soweit feststellbar – an die jeweils zuständigen nationalen Strafverfolgungsbehörden übersandt.

Das Ziel dieser Verordnung, die Bekämpfung des sexuellen Missbrauchs von Kindern, ist vollkommen unstreitig und ohne jeden Zweifel ein wichtiges Anliegen. Auch ich halte es für geboten, den Schutz der Opfer dadurch zu gewährleisten, dass Täter aus der Anonymität des Netzes herausgeholt, gezielt ermittelt und ihrer Bestrafung zugeführt werden.

Auch der wichtigste Zweck heiligt aber nicht den Einsatz aller denkbaren Mittel. Nach meiner Auffassung schießt der Verordnungsentwurf deutlich über das Ziel hinaus.

Entsprechend ist er in der öffentlichen Diskussion auf erhebliche Kritik gestoßen. Ablehnung erfährt er nicht nur von Seiten der Datenschutzbeauftragten, sondern auch von Vertretern der Opferschutzorganisationen wie etwa dem Kinderschutzbund und dem Deutschen Kinderverein.

Diese Kritik teile ich. Denn der Verordnungsentwurf verstößt gegen elementare rechtsstaatliche Grundsätze.

Es bestehen schon erhebliche Zweifel, dass die Vorgaben der Verordnung technisch überhaupt umsetzbar sind.

Gerade Chat-Dienste wie WhatsApp bieten regelmäßig eine Ende-zu-Ende-Verschlüsselung der Kommunikation an; sie verfügen mithin gar nicht über die technische Möglichkeit, die über ihren Dienst ausgetauschten Inhalte zu überprüfen. Der Verordnungs-Entwurf setzt sich mit dieser Problematik nicht auseinander.

Eine Software, die neue kinderpornographische Aufnahmen sicher erkennt und von belanglosen Aufnahmen mit nackter Haut unterscheidet, dürfte es zudem - jedenfalls derzeit - noch nicht geben. Noch viel weniger besteht die Möglichkeit, allein aufgrund einer IT-gesteuerten Textanalyse festzustellen, ob eine Person in einer Kommunikation darauf abzielt, ein Kind letztlich sexuell zu missbrauchen.

Wenn eine Mutter ein Bild ihres nackten Kleinkinds in der Badewanne oder am Strand an dessen Großeltern verschickt, verbreitet sie damit kein kinderpornographisches Material. Es ist allerdings zweifelhaft, ob eine Software diesen Unterschied sicher zu erkennen vermag.

Es steht daher zu befürchten, dass die Massenüberwachung zu zahllosen - auch falschen - Meldungen führen wird. Deren händische Überprüfung durch eine zentrale Behörde in der EU dürfte – wenn sie denn überhaupt zu leisten ist - einen ganz erheblichen Zeit- und Personalaufwand mit sich bringen.

Der Regelungsentwurf begegnet aber vor allem unter rechtlichen Aspekten ganz grundlegenden Bedenken.

Er ermöglicht auf der Grundlage abstrakter Risikobewertungen eine anlasslose Massenüberwachung aller Nutzer einer bestimmten App oder eines bestimmten E-Mail-Dienstes.

Niemand käme auf den Gedanken, sämtliche Briefe der Post öffnen und lesen zu lassen, wenn Erkenntnisse bestünden, dass diese von einzelnen Kunden für die Versendung von kinderporno- graphischem Material genutzt wird.

Derart unverhältnismäßige Eingriffe in Grundrechte der Bürgerinnen und Bürger sind nicht zu rechtfertigen. Das ändert sich auch nicht dadurch, dass das Fortschreiten der Technik es möglicherweise erleichtert, die Kommunikation via Internet flächendeckend zu überwachen.

Das Fernmeldegeheimnis des Artikel 10 Grundgesetz schützt jede unkörperliche Übermittlung von Informationen an individualisierte Empfänger mit Hilfe des Telekommunikationsverkehrs, und somit auch die Kommunikation mittels E-Mail, Chat oder SMS. Dabei schützt es vor allem den Inhalt der vertraulichen Kommunikation. Muss der Einzelne fürchten, dass Dritte Einblick in seine vertrauliche Kommunikation nehmen, verändert das sein Kommunikationsverhalten. Er verhält sich nicht mehr frei.

Insoweit kommt auch eine Beeinträchtigung des Rechts auf informationelle Selbstbestimmung aus Artikel 2 Absatz 1 in Verbindung mit Artikel 1 Absatz 1 Grundgesetz in Betracht. Eine freie und ungestörte Kommunikation ist nämlich elementarer Bestandteil der für einen Rechtsstaat erforderlichen freien Persönlichkeitsentfaltung seiner Bürgerinnen und Bürger.

Das Fernmeldegeheimnis ist nicht uneingeschränkt gewährleistet. Eingriffe in dieses Recht müssen aber dem Grundsatz der Verhältnismäßigkeit entsprechen, wobei gerade Inhalte, die dem Kernbereich privater Lebensgestaltung zuzurechnen sind, einen besonderen Schutz genießen. Diesen Anforderungen genügen die vorgeschlagenen Regelungen meines Erachtens nicht.

Die Masse der betroffenen Nutzer hat durch ihr Verhalten keinerlei Anlass dafür gegeben, dass die Inhalte ihrer Kommunikation auf staatliche Anordnung hin durchsucht und ausgewertet werden. Gegen sie besteht, um es in Begriffen des Strafverfahrensrechts auszudrücken, keinerlei Anfangsverdacht. Gleichwohl

sollen rein abstrakte Risiken ausreichend sein, um den Inhalt ihrer privaten Kommunikation und der aller User eines bestimmten Messengerdienstes quasi mit einem großen Staubsauger zu sammeln und auszuwerten. Die Wahrscheinlichkeit, in diesem riesigen Datenberg neues kinderpornographisches Material zu finden, dürfte im Vergleich zu den vielen hunderten oder gar tausenden Eingriffen in die Grundrechte unbescholtener Bürgerinnen und Bürger gering und der Eingriff mithin nicht vertretbar sein.

Ein solches Vorgehen birgt zudem das Risiko, dass Bürgerinnen und Bürger ihr Vertrauen in den Schutz privater Kommunikation und damit auch in den Rechtsstaat verlieren könnten.

Die Verordnung dürfte überdies mit den Vorgaben des Europäischen Gerichtshofs nicht in Einklang zu bringen sein. Dieser hat immer wieder betont, dass die europäische Richtlinie über die Verarbeitung und den Schutz der Privatsphäre in der elektronischen Kommunikation die Mitgliedstaaten verpflichtet, die Vertraulichkeit der mit öffentlichen Kommunikationsdiensten übertragenen Nachrichten sicherzustellen. Die Richtlinie erlaube es den Mitgliedstaaten zwar - unter anderem auch zu Zwecken der Kriminalitätsbekämpfung - hiervon Ausnahmen vorzusehen; diese müssten aber verhältnismäßig und auf das absolut Notwendige beschränkt sein.

Die im Verordnungsentwurf vorgesehenen Maßnahmen dürften dem nicht genügen. Aufgrund der skizzierten technischen Schwierigkeiten dürften die vorgesehenen Maßnahmen zur Erreichung des Zieles schon nicht geeignet sein.

Sie sind aber auch nicht erforderlich, denn es gibt weniger eingriffsintensive, zielgerichtetere und damit auch effektivere Maßnahmen, um Kinderpornographie zu bekämpfen, als die vollständige Inhaltskontrolle der Kommunikation zahlloser Menschen, die durch ihr Verhalten hierzu keinerlei Anlass gegeben haben.

Der Europäische Gerichtshof hat wiederholt, zuletzt in seinem Urteil zu den irischen Vorschriften der Vorratsdatenspeicherung vom 5. April 2022, eine

Möglichkeit aufgezeigt, wie die Strafverfolgungsbehörden in rechtlich zulässiger Art und Weise vorgehen können, um solche Täter im Internet zu identifizieren, nämlich durch Zugriff auf die den Internet-Protokoll-Daten – der sogenannten IP-Adresse - zugeordneten Anschlussdaten.

Aktuell müssen Ermittlungsverfahren wegen Besitzes oder Verbreitens von Kinderpornographie über das Internet wiederholt eingestellt werden, weil der oder die Täter nicht ermittelt werden können. Zwar liegt den Ermittlern möglicherweise die IP-Adresse eines Anschusses vor, über den kinderpornographisches Material von einem Server herunter- oder auf einen Server hochgeladen wurde. Der Anschlussinhaber lässt sich aber nur ermitteln, wenn der Internet-Provider noch die Daten gespeichert hat, aus denen sich ergibt, welchem Anschluss die verwendete IP-Adresse zu einem bestimmten Zeitpunkt zugeordnet war. Zur Speicherung solcher Daten besteht aber derzeit keine Verpflichtung, da die gesetzlichen Regelungen zur Verkehrsdatenspeicherung seit einer Entscheidung des Oberverwaltungsgerichts Münster von Juni 2017 faktisch ausgesetzt sind.

Ermittlungserfolge lassen sich in diesem Bereich daher derzeit nur erzielen, wenn die Provider diese Daten freiwillig zu anderen Zwecken gespeichert haben. Das ist in aller Regel höchstens für einen Zeitraum von zwei bis maximal sieben Tagen der Fall. Entsprechende Ermittlungen sind mithin sehr zeitkritisch und daher leider wiederholt erfolglos.

Der Europäische Gerichtshof hat ausdrücklich ausgeführt, dass es zur Bekämpfung schwerer Kriminalität, zu der der sexuelle Missbrauch von Kindern zweifellos gehört, sowohl zulässig sei, IP- Adressen allgemein und unterschiedslos auf Vorrat zu speichern wie auch die Daten, aus denen sich die Identität der Nutzer elektronischer Kommunikationsmittel ergeben.

Dies würde die Aufklärungsmöglichkeiten erhöhen. Gerade kinderpornographisches Material wird häufig von Tätern anonym über das Netz getauscht. Jeder Tausch hinterlässt eine Spur in Form einer IP-Adresse. Lässt

sich diese noch für einen längeren Zeitraum retrograd einem Anschluss zuordnen, so würde die Ermittlung eines Täters und die Auswertung seiner IT dazu führen, dass in der Folge zahlreiche weitere Verfahren eingeleitet und Täter ermittelt werden könnten.

Derartig zielgerichtete und anlassbezogene Maßnahmen sind zur Bekämpfung des sexuellen Missbrauchs von Kindern deutlich geeigneter und weniger eingriffsintensiv als der naiv anmutende Versuch, Unmengen an inhaltlicher Kommunikation unbescholtener Bürgerinnen und Bürger in der Hoffnung zu durchforsten, dabei eventuell auf Kinderpornographie zu stoßen.

Die Annahme der zuständigen EU- Innenkommissarin, in diesem riesigen Heuhaufen von Daten die richtigen Stecknadeln zu finden, ist trügerisch. Ich halte es für richtiger und zielführender, erst gar nicht dort suchen zu müssen, sondern passgenaue Möglichkeiten zur Identifizierung des oder der Täter auszuschöpfen.

Anzumerken ist, dass das Gesetzgebungsverfahren auf europäischer Ebene mit der Vorlage des Verordnungsentwurfs durch die EU-Kommission erst begonnen hat. Sowohl die Mitgliedstaaten als auch das Europäische Parlament werden umfassend Gelegenheit haben, sich hier inhaltlich einzubringen. Der weitere Verlauf der Verhandlungen ist daher abzuwarten.

Sowohl der Bundesjustizminister als auch die Bundesinnenministerin haben sich bereits kritisch bzw. ablehnend zu dem aktuellen Regelungsvorschlag geäußert. Es besteht daher die Hoffnung, dass er – zumindest in dieser Form – nicht in Kraft treten wird.

Lassen Sie mich kurz zusammenfassen:
Die Aufklärung und auch die Verhinderung des sexuellen Missbrauchs von Kindern muss mit allen rechtsstaatlichen Mitteln betrieben werden.

Pauschal die private Kommunikation zahlloser Bürgerinnen und Bürger über das Internet unter einen Generalverdacht zu stellen, ist hierfür aber kein geeignetes Mittel.“

Mit freundlichen Grüßen

Herbert Mertin