Markus Ferber, MdEP
ist Vorsitzender der Hanns-Seidel-Stiftung, München, und Koordinator im Wirtschafts- und Währungsausschuss des Europäischen Parlaments, der sich auch mit dem Digital Services Act beschäftigt.

Markus Ferber

/// Ein Beitrag zur Bekämpfung von Missbrauchsdarstellungen im Netz

Das Konzept des Digital Services Act

Kindesmissbrauch ist eines der schlimmsten Verbrechen. Deshalb steht die Politik in einer besonderen Verantwortung, alles Mögliche dafür zu tun, Kindesmissbrauch offline wie online zu verhindern. Dieser Artikel wagt eine Einordnung eines insbesondere europäischen Problems und zeigt auf, was bereits geschieht respektive noch geschehen muss.

Ein europäisches Problem

Kindeswohl hat höchste Priorität. Umso erschreckender ist es, dass Materialien zum sexuellen Missbrauch von Kindern, Child Sexual Abuse Material (CSAM), auch 10 Jahre nach dem Inkrafttreten der Richtlinie 2011/92/EU[1] zur Bekämpfung des sexuellen Missbrauchs und der sexuellen Ausbeutung von Kindern sowie der Kinderpornografie immer häufiger im Internet zu finden sind.

Trotz der staatlichen Bemühungen nehmen Missbrauchsdarstellungen im Netz zu.

So weist die Europäische Kommission beispielsweise in ihrer kürzlich veröffentlichten Mitteilung[2] auf den dramatischen Anstieg der Berichte über sexuellen Kindesmissbrauch im Internet in Europa, und speziell während der COVID-19-Pandemie, hin. Belegt wird dies durch Zahlen der Internet Watch Foundation (IWF), die jährlich Statistiken über die Anzahl der Hosting-URLs, die kinderpornografische Inhalte aufweisen, veröffentlicht. So zeigt der Jahresbericht 2019[3] ein alarmierendes Bild: 89 % der bekannten URLs, die Material über sexuellen Kindesmissbrauch enthalten, wurden in Europa gehostet. Europäischer Spitzenreiter sind die Niederlande, deren

Hosting-Aktivitäten 71 % der weltweit entdeckten Menge ausmachten. Zurückzuführen ist dies insbesondere auf das Geschäftsmodell des „kugelsicheren Hostings", das die Vorteile des freizügigeren Rechtssystems und der technischen Infrastruktur in den Niederlanden nutzt. Gefolgt werden die Niederlande in Europa von Frankreich, der Slowakei, Lettland, Deutschland, Bulgarien und Rumänien.[4] Mit weitem Abstand hinter Europa folgt Nordamerika, wo 9 % aller bekannten URLs mit Inhalten zu sexuellem Kindesmissbrauch gehostet wurden.

Der Corona-Lockdown hat die Zahl der potenziellen Opfer erhöht.

Dieses Phänomen hat sich im vergangenen Jahr durch die Corona-Pandemie verstärkt. Während des Corona-Lockdowns verlagerte sich das Leben vieler Kinder noch weiter von der realen in die virtuelle Welt. Sexualstraftäter haben in dieser Entwicklung eine verlockende Möglichkeit gefunden, sich einen größeren Kreis potenzieller Opfer zu erschließen. So weist das Internet Organised Crime Threat Assessment[5] von EUROPOL während des COVID-19-Lockdown-Zeitraums einen signifikanten Anstieg der Aktivitäten im Zusammenhang mit sexuellem Missbrauch und Ausbeutung von Kindern sowohl im Surface Web als auch im Dark Web auf.

Vor diesem Hintergrund möchte ich eine kurze Einordnung der bisherigen Zusammenarbeit innerhalb und außerhalb der EU, insbesondere hinsichtlich ihrer EU-Agenturen, wagen. Gleichzeitig werde ich auch die Möglichkeiten des Digital Services Act (DSA)[6] aufzeigen, welcher neue Vorschriften für Vermittlungs- und Hosting-Dienste, Online-Plattformen und strengere Regeln für sehr große Online-Plattformen (wie beispielsweise Google, Amazon, Facebook, Apple und Microsoft) vorsieht.

Zusammenarbeit in Europa und weltweit

Das gezielte Filtern und das Verfolgen von kinderpornografischen Inhalten durch Service- und Plattformbetreiber ist bis heute freiwillig. Grund dafür sind unter anderem die strengen Datenschutzbestimmungen in Europa.[7]

Umso wichtiger scheint es, die Bemühungen der EU-Institutionen, ihrer Agenturen als auch den mit ihnen verbundenen öffentlich-privaten Partnerschaften und internationalen Kooperationen zu intensivieren, bis eine rechtlich klare und verpflichtende Grundlage geschaffen ist.

Ein wichtiger Meilenstein dafür war die im vergangenen Jahr verabschiedete EU-Strategie für eine wirksamere Bekämpfung des sexuellen Missbrauchs von Kindern.[8] Hinzu kommt aber auch die in diesem Jahr verabschiedete

EU-Strategie für die Rechte des Kindes.[9] Aufbauend auf diesen Strategien und der bereits im Jahr 2011 verabschiedeten Richtlinie 2011/92/EU[10] arbeiten die EU-Institutionen eng mit ihren EU-Agenturen für Strafverfolgung und justizielle Zusammenarbeit – EUROPOL und EUROJUST – und anderen Akteuren zusammen.

So fällt die sexuelle Ausbeutung von Kindern bei Online- wie Offline-Delikten in den Zuständigkeitsbereich von EUROPOL.[11] Im Januar 2013 wurde deshalb das Europäische Zentrum für Cyberkriminalität (EC3) gegründet, welches Cyberkriminalität, insbesondere im Zusammenhang mit der sexuellen Ausbeutung von Kindern im Internet, bekämpft. Darüber hinaus beteiligt sich EUROPOL an Initiativen wie der European Financial Coalition against Commercial Sexual Expoitation of Children Online (EFC), der Virtual Global Taskforce (VGT), der Victim Identification Taskforce, dem Projekt HAVEN sowie der „Trace an Object"-Initiative, um immer mehr Opfer und ihre Missbraucher zu identifizieren.[12]

Seit seiner Gründung im Jahr 2002 hat auch EUROJUST[13] in enger Zusammenarbeit mit anderen Stakeholdern eine aktive Rolle bei der Bekämpfung von Verbrechen gegen Kinder eingenommen. So ist EUROJUST ebenfalls Mitglied der EFC und fungiert dort als Anlaufstelle und Kompetenzzentrum für schwere grenzüberschreitende Straftaten gegen Kinder. Mit der Gründung des European Judicial Cybercrime Network (EJCN) im Jahr 2016 übernahm EUROJUST dabei auch wichtige Koordinierungsfunktionen und unterstützt seither die Mitglieder bei der Umsetzung des Arbeitsprogramms.[14]

Europäische und Internationale Kooperationen koordinieren die Bekämpfung von Verbrechen an Kindern.

In diesem Zusammenhang sind die Europäischen Institutionen und ihre Agenturen in verschiedensten öffentlich-privaten Partnerschaften und internationalen Kooperationen engagiert. So arbeiten sie eng mit dem INHOPE network of hotlines[15] zusammen. In der Alliance to Better Protect Minors Online[16] kommen die Europäische Kommission, führende IKT- und Medienunternehmen, Nichtregierungsorganisationen und UNICEF zusammen, um das Internet für Kinder und Jugendliche grundlegend zu verbessern, ihre „digital literacy" zu stärken und eine bessere Bewusstseinsbildung zu fördern. Durch EU-Mittel gefördert wird beispielsweise auch die WeProtect Global Alliance to End Child Sexual Exploitation Online,[17] eine Multi-Stakeholder-Organisation, die 98 Regierungen, 41 Unternehmen, 44 zivilgesellschaftliche Organisationen und internationale Institutionen vereint. ECPAT International stellte darüber hinaus im Jahr 2020 eine detaillierte Analyse zur sexuellen Ausbeutung von Kindern im Internet sowie den wichtigsten Herausforderungen und Trends vor und skizziert weitere Beispiele für die Zusammenarbeit von Strafverfolgungsbehörden und privaten Akteuren auf internationaler Ebene.[18]

Technologische Entwicklungen wie PhotoDNA verhindern die Verbreitung kinderpornografischer Inhalte.

Insbesondere hervorzuheben ist dabei der Erfolg von technologischen Entwicklungen wie PhotoDNA, einer im Jahr 2009 von Microsoft und dem Dartmouth College entwickelten Technologie.[19] Dabei handelt es sich um ein automatisiertes System, das einem Bild mit kinderpornografischen Inhalten einen „hash", d. h. einen eindeutigen digitalen Fingerabdruck, zuweist. Dadurch können weitere Kopien, auch wenn sie bearbeitet wurden, automatisch erkannt und an der Verbreitung gehindert werden. Ähnliche Technologien gibt es auch für Video-Sharing-Plattformen (VSPs), die es den Plattform-Betreibern wie Microsoft, Google, Twitter, Facebook, Adobe Systems und Reddit erlauben, CSAM-Inhalte zu identifizieren und zu entfernen, überwiegend, bevor sie von einem Nutzer gesehen werden.[20]

Der DSA und die Bekämpfung illegaler Online-Inhalte

In Zusammenspiel mit diesen Aktivitäten legt der Kommissionsvorschlag zum DSA einen horizontalen Rahmen für Transparenz, Rechenschaftspflichten und die regulatorische Aufsicht zur Bekämpfung von illegalen Online-Inhalten für den EU-Online-Raum fest (Artikel 2).[21]

Der Entwurf des DSA gilt dabei für Online-Vermittlungsdienste und sieht für verschiedene Kategorien von Unternehmen, je nach Rolle, Größe und Wirkung im Online-Ökosystem, unterschiedliche Verpflichtungen vor. In diesem Zusammenhang gibt es insbesondere drei Mechanismen, die es mittels des DSA erlauben würden, illegale Inhalte im Internet zu bekämpfen.

Erstens sieht der Vorschlag ein sogenanntes „notice and take down"-Verfahren vor, welches Online-Plattformen als auch Hosting-Anbieter dazu verpflichten soll, Melde- und Aktionsmechanismen einzurichten, die es Dritten ermöglichen, das Vorhandensein mutmaßlich illegaler Inhalte zu melden (Artikel 14) und im Anschluss die Plattformen dazu verpflichtet, diese Inhalte zu überprüfen und aus dem Netz zu nehmen.

Zweitens führt der Vorschlag auch das Konzept der „trusted flaggers" ein. Diese sind von den Behörden der Mitgliedstaaten benannte Stellen mit besonderer Sachkenntnis und Kompetenz im Umgang mit illegalen Inhalten. Online-Plattformen wären dann verpflichtet, Hinweise dieser „trusted flagger" vorrangig zu bearbeiten (Artikel 19) und müssten die zuständigen Strafverfolgungsbehörden informieren, wenn sie Kenntnis von Informationen erhalten, die den Verdacht auf schwere Straftaten mit einer Bedrohung für das Leben oder die Sicherheit von Menschen begründen (Artikel 21).

Drittens würden mit dem DSA strengere Auflagen für sehr große Online-Plattformen wie beispielsweise Facebook, Google oder Twitter eingeführt werden, die mehr als 45 Millionen aktive Nutzer in der EU pro Monat haben. Dabei müssten diese „very large online platforms“ (VLOPs) mindestens einmal jährlich die systemischen Risiken bewerten, die sich aus dem Betrieb und der Nutzung ihrer Dienste ergeben (Artikel 26), einschließlich des potenziellen Missbrauchs durch Nutzer ihrer Dienste, zum Beispiel bei der Verbreitung illegaler Inhalte wie Material zum sexuellen Missbrauch von Kindern.

Im Anschluss an eine solche Analyse wären VLOPs verpflichtet, geeignete Abhilfemaßnahmen zu ergreifen (Artikel 27) wie z. B. die Anpassung des Designs und der Funktionsweise ihrer Inhaltsmoderation, ihrer Algorithmen oder Online-Schnittstellen, damit die Verbreitung von illegalen Inhalten erfolgreich verhindert und einschränkt werden kann. Bei einer etwaigen Nichteinhaltung (Artikel 58) kann die Kommission unter anderem Geldbußen (Artikel 59) und Zwangsgelder (Artikel 60) für Verstöße gegen die Verordnung erlassen.

Schlussfolgerungen

Diese neuen Vorschriften sind ein erster Schritt in die richtige Richtung und könnten dazu beitragen, neben der Stärkung einer gesellschaftlichen „Kultur des Hinsehens“ adäquate Schnittstellen zwischen den beteiligten Akteuren sowie den dahinterliegenden Prozessen und Aufsichtsbehörden zu etablieren respektive zu vertiefen.

Das Thema Haftungsfragen von Online-Plattformen hat einen großen Diskussionsbedarf.

Was diese Maßnahmen allerdings verbergen, ist eine weitgreifende und durchaus notwendige Debatte, die in den Rechtswissenschaften, beispielsweise bei der Haftungsfrage von Online-Plattformen, schon länger geführt wird.[22] Im Kern geht es dabei darum, ob Soft-Law- und User-Empowerment-Initiativen, auf die auch der DSA setzt, der richtige Weg sind, um sexuellen Missbrauch und die Verbreitung von Missbrauchsdarstellungen im Internet zu bekämpfen. Ich plädiere dafür, dass wir uns diesem Problem aus drei Richtungen annähern.

Einerseits müssen wir die zivilgesellschaftliche Aufmerksamkeit als auch das zivilgesellschaftliche Engagement fördern und fordern. Dies gelingt nur, wenn wir die breite Öffentlichkeit für das Thema durch gezielte Kampagnen sensibilisieren. Es darf nicht sein, dass der Aufschrei wie nach dem Missbrauchsskandal in Münster[23] groß ist, nach kurzer Zeit aber wieder abebbt. Wir brauchen nachhaltige und konsequente Informations- und Aufklärungspolitik, die durch öffentliche Mittel gefördert wird.

Wir werden die Strafverfolgungskapazitäten auf internationaler Ebene weiter stärken.

Andererseits befinden wir uns zwar organisatorisch und in der europaweiten Zusammenarbeit auf einem guten Weg, müssen unsere Bemühungen bei gleichzeitig steigenden Kindesmissbrauchsmaterialien im Netz aber noch weiter intensivieren. Die Investitionsbudgets der Mitgliedstaaten als auch der EU bieten hierfür Mittel, um Waffengleichheit herzustellen. Dies gilt insbesondere bei der Aus- und Aufrüstung der nationalen als auch supranationalen Strafverfolgungsbehörden, sei es bei den dafür notwendigen digitalen Fertigkeiten oder angemessener Soft- oder Hardware. Auch eine verpflichtende Einführung von Anwendungen wie PhotoDNA unter Schnittstellenkontrolle durch die kompetenten EU-Agenturen könnte dazu beitragen.

Letztlich müssen wir auch die Neujustierung der rechtlichen Handlungsoptionen und Rahmenbedingungen überdenken. Einerseits könnte dies beispielsweise ein Vertragsverletzungsverfahren gegen die Niederlande sein, andererseits auch die oben angedeutete gesetzliche Verpflichtung zur Einführung zielgerichteter Abhilfemaßnahmen. Sicherlich birgt die damit einhergehende Debatte Gefahr, durch die Angst vor einem generalisierten Upload-Filter oder dem „Überwachungsstaat" überlagert zu werden, allerdings haben Applikationen wie PhotoDNA ihre zielgerichtete Wirksamkeit und Anwendbarkeit bereits bewiesen. Der technologische Fortschritt ist auch hier unaufhaltsam und ich bin überzeugt, dass man die Kräfte des Marktes und die Macht der Politik dazu nutzen kann, um letztendlich den gesetzlichen verbindlichen Schutz von Kindern zur Bekämpfung von Missbrauchsdarstellungen im Netz festzuschreiben.

///

Anmerkungen

1 RICHTLINIE 2011/92/EU: Richtlinie 2011/92/EU des Europäischen Parlaments und des Rates vom 13. Dezember 2011 zur Bekämpfung des sexuellen Missbrauchs und der sexuellen Ausbeutung von Kindern sowie der Kinderpornografie sowie zur Ersetzung des Rahmenbeschlusses 2004/68/JI des Ra., Brüssel 2011.

2 COM(2020) 607 final: Mitteilung der Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen. EU-Strategie für eine wirksamere Bekämpfung des sexuellen Missbrauchs von Kindern, Brüssel 2020.

3 Internet Watch Foundation (IWF): IWF 2019 Annual Report, Cambridge 2019.

4 INHOPE: Annual Report 2019, Amsterdam 2019.

5 EUROPOL: Internet organised crime threat assessment (IOCTA) 2020, Den Haag 2020.

6 COM(2020) 825 final: Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über einen Binnenmarkt für digitale Dienste (Gesetz über digitale Dienste) und zur Änderung der Richtlinie 2000/31/EG, Brüssel 2020.

7 RICHTLINIE 2002/58/EG: Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation), Brüssel 2002; VERORDNUNG (EU) 2016/679: Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG, Brüssel 2016; VERORDNUNG 2017/0003 (COD): Verordnung des Europäischen Parlaments und des Rates über die Achtung des Privatlebens und den Schutz personenbezogener Daten in der elektronischen Kommunikation und zur Aufhebung der Richtlinie2002/58/EG, Brüssel 2017; COM(2020) 568 final: Vorläufige Verordnung über die Verarbeitung personenbezogener und anderer Daten zum Zweck der Bekämpfung des sexuellen Missbrauchs von Kindern, Brüssel 2020.

8 COM(2020) 607 final.

9 COM(2021) 142 final: Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: EU strategy on the rights of the child, Brüssel 2021.

10 RICHTLINIE 2011/92/EU.

11 EUROPOL: European Cybercrime Centre (EC3), Brüssel 2021.

12 EUROPOL: Child Sexual Exploitation, Brüssel 2021.

13 EUROJUST: Crimes against children, Den Haag 2021; EUROJUST: European Union Agency for Criminal Justice Cooperation, Den Haag 2021.

14 Ebd.; European Judicial Cybercrime Network (EJCN): European Judicial Cybercrime Network, Den Haag 2021.

15 INHOPE: Inhope Webpage, Amsterdam 2021.

16 Europäische Kommission: Alliance to better protect minors online, Brüssel 2021.

17 WeProtect: A global coalition to fight child sexual exploitation and abuse online, 2021.

18 ECPAT International: Summary Paper Online Child Sexual Exploitation, 2020.

19 Microsoft: Help stop the spread child sexual exploitation and abuse online, 2009.

20 SMART 2018/0066: Study on the implementation of the new provisions in the revised Audiovisual Media Services Directive (AVMSD), Brüssel 2020.

21 COM(2020) 825 final.

22 European Parliamentary Research Service (EPRS): Liability of online platforms, Brüssel 2021.

23 Landgericht Münster: Missbrauchsprozess, Münster 2021.