Positionspapier der kinderschutzpolitischen Sprecherinnen und Sprecher von CDU und CSU in den deutschen Landtagen und Bürgerschaften sowie dem Abgeordnetenhaus von Berlin

Thema: Polizei und Strafverfolgung

Einleitung

Laut der Polizeilichen Kriminalstatistik (PKS) für das Jahr 2020 werden in Deutschland täglich durchschnittlich 46 Kinder sexuell missbraucht, was einen Zuwachs von 6,8% im Vergleich zum Vorjahr in diesem Deliktsfeld bedeutet. Dabei handelt es sich allerdings nur um das so genannte Hellfeld, also die Anzahl der bei der Polizei erfassten Straftaten. Die Dunkelziffer dürfte deutlich höher liegen. Das Bundesministerium der Justiz und für Verbraucherschutz schätzte das Dunkelfeld beim sexuellen Missbrauch im Jahr 2018 achtmal so groß ein, wie die der Justiz bekannt gewordenen Fälle.

Dieses Positionspapier fasst die Erkenntnisse des im Rahmen der ersten Sprechertagung in Düsseldorf am 4./5. Oktober 2021 stattgefundenen Besuchs beim Landeskriminalamt Nordrhein-Westfalen (LKA NRW) zusammen.

Relevanz des Themas

Durch die extrem schnell wachsende Präsenz des Internets erleben Kinder und Jugendliche auch in der digitalen Welt massive Gewalt, insbesondere auch sexuellen Missbrauch. Das Internet ist heute wesentlicher „Handlungsort“ von Missbrauchstaten. Als CDU- und CSU-Landtagsfraktionen ist es uns ein zentrales Anliegen, unsere Polizei und Strafverfolgungsbehörden mit allen technisch notwendigen Instrumenten auszustatten, die es ihnen ermöglichen, Täterinnen und Täter im Internet noch effektiver aufspüren zu können. Laut PKS ist die Zahl der gemeldeten Fälle des Besitzes, der Herstellung und der Verbreitung von Missbrauchsabbildungen von Kindern und Jugendlichen bundesweit im Jahr 2020 um 53% gegenüber dem Vorjahr gestiegen. In Nordrhein-Westfalen kam es in dem genannten Zeitraum sogar zu einer Steigerung von 102,5%.

Schätzungen zufolge werden mit Missbrauchsabbildungen global jährlich zwischen drei und 20 Mrd. US-Dollar umgesetzt. Millionen Menschen greifen auf Missbrauchsabbildungen zu. Zwischen 50.000 und 100.000 Pädokriminelle sind weltweit in organisierten Pornoringen aktiv. Schätzungen aus dem Jahr 2001 gingen davon aus, dass zu jeder Zeit mehr als eine Million pornografische Bilder von Kindern im Internet existieren und dass ungefähr 200 neue Bilder/Videos täglich veröffentlicht werden. Gut 20 Jahre später dürften diese Zahlen um ein Vielfaches höher ausfallen!

Der enorme Anstieg der Anzahl der erfassten Fälle wegen Missbrauchsabbildungen in Nordrhein-Westfalen und bundesweit ist auch auf die gesteigerten Aktivitäten der Polizei sowie eine deutliche Zunahme von Meldungen zu Missbrauchsabbildungen im Internet zurückzuführen. Trotz dieser grundsätzlich positiven Entwicklung stehen nach wie vor zahlreiche rechtliche Hürden einer noch effektiveren Strafverfolgung entgegen. Im Folgenden werden die Herausforderungen und Hemmnisse in der Ermittlungsarbeit dargestellt sowie konkrete Lösungsansätze aus Sicht der CDU/CSU-Fraktionen in den Ländern aufgezeigt.

Verkehrsdatenspeicherung

Laut BKA konnten alleine im Jahr 2017 8.400 von insgesamt 36.900 Verdachtshinweisen des National Center for Missing & Exploited Children (NCMEC) nicht aufgeklärt werden, da die jeweiligen deutschen IP-Adressen mangels Umsetzung der Verkehrsdatenspeicherung keinen konkreten Personen mehr zugeordnet werden konnten. Das entspricht einer Quote von 22,75%. Der Grund für die fehlende Umsetzung liegt hierbei nicht in einer gesetzlichen Regelungslücke, sondern in einem Vollzugsdefizit. Derzeit ist die Verkehrsdatenspeicherung aus dem Jahr 2017 in Deutschland durch die Bundesnetzagentur unter Verweis auf die europäische Rechtsprechung faktisch ausgesetzt. Der Europäische Gerichtshof (EuGH) hat im Oktober 2020 in seinem Urteil jedoch ausdrücklich betont, dass von einem Verbot der anlass- und unterschiedslosen Speicherung von Verkehrs- und Standortdaten abgewichen werden kann, wenn entweder eine ernsthafte Bedrohung der nationalen Sicherheit vorliegt oder wenn sie der Bekämpfung schwerer Straftaten dient.

Zur Durchsetzung der polizeilichen Aufträge zur Gefahrenabwehr und zur Strafverfolgung im Internet müssen digitale Ermittlungsansätze (IP-Adressen) allerdings einen längeren Zeitraum vorgehalten werden, damit diese in begründeten Fällen erhoben, gesichert und ausgewertet werden können. Andernfalls sind Identifizierungen von Täterinnen und Tätern und/oder gefahrenabwehrende Maßnahmen wesentlich erschwert oder gar verhindert. In der Regel dauert es 10 bis 20 Tage, bis es zu einer Anzeigeerstattung eines Opfers kommt. Unter den deutschen Providern existieren (wenn überhaupt) im Festnetz aktuell sehr unterschiedliche Speicherfristen, maximal jedoch sieben Tage. Eine Identifizierung ist nur mit hoher technischer Expertise und unter Mitwirkung der Provider möglich. Dies führt zu einer langen Verfahrensdauer für Verfahren mit Kindesmissbrauch, was wiederum eine zusätzliche Belastung und Traumatisierung der Opfer zur Folge hat. Einheitliche und längere Speicherfristen wären aus unserer Sicht der richtige Weg. Eine Speicherung von 10 Wochen, wie es die derzeitige Rechtslage in § 113b TKG vorsieht, aber wie erwähnt derzeit nicht erfolgt, würde den Ermittlerinnen und Ermittlern einen immensen Vorteil bei der Strafverfolgung bringen. Dabei sollte es ausdrücklich nicht um eine allumfassende Speicherung gehen, wer, wann, welche Webseite besucht hat. Vielmehr sollte lediglich zum Zwecke der Strafverfolgung die Abfrage von IP-Adressen und deren Zuordnung zu einem konkreten Gerät ermöglicht werden, um anschließend zu prüfen, welche Person bei einem konkreten Verdachtsfall das entsprechende Gerät genutzt hat.

Die für die Aufsicht und Durchsetzung der Verkehrsdatenspeicherung zuständige Bundesnetzagentur hat verwaltungsgerichtliche Urteile zum Anlass genommen, Verstöße der Provider nicht zu sanktionieren. Dieser rechtliche Schwebezustand muss zügig beendet und eine abschließende Entscheidung getroffen werden. Wir sprechen uns für eine bundesweit einheitliche Handhabung aus, die unter Beachtung der Vorgaben des EuGH den erfolgreichen Einsatz der Nutzung von Verkehrsdaten zum Zwecke der Verfolgung schwerer Kriminalität, insbesondere der sexualisierten Gewalt gegen Kinder und Jugendliche, ermöglicht. Sollte eine umfassende Umsetzung zeitnah nicht möglich sein, wäre ggf. auch eine (Teil-) Umsetzung zu prüfen, welche sich zunächst auf Verfahren wegen sexuellen Missbrauchs und Missbrauchsabbildungen (von Kindern und Jugendlichen) beschränkt.

Verhinderung anonymer Chats

Das Internet ermöglicht Fremden, die sich hinter einem Computerbildschirm und gefälschten Identitäten verstecken, einen einfachen und anonymen Zugang zu Kindern und Jugendlichen. Analog zur „realen Welt“ müssen daher auch im Internet Schutz- und Sicherheitsmechanismen implementiert sein. Chat-Accounts sollten beispielsweise nur am Chatgeschehen teilnehmen können, wenn diese mittels einer deutschen Rufnummer („+49“) registriert sind. Da in Deutschland die Registrierung neuer Rufnummern über ein IDENT Verfahren läuft, würde dies den Strafverfolgungsbehörden in der Regel ermöglichen, die Täterinnen und Täter zu identifizieren, und gleichzeitig die täterseitige Hemmschwelle erhöhen. Pseudonyme innerhalb des Chats sollten weiterhin möglich sein.

Verifikation durch Eltern

Kinder können heute ohne großen Aufwand und Kontrolle der Eltern einen Chat-Account anlegen. Dabei müssen sie zum Teil lediglich per Knopfdruck bestätigen, dass sie ein bestimmtes Alter haben, z.B. über eine einfache E-Mail-Bestätigung. Zum Schutz der Kinder vor Übergriffen in Chats sollten Unternehmen ihre Systeme darauf ausrichten, dass Eltern für ihre minderjährigen Kinder bürgen bzw. bestätigen müssen, dass die Teilnahme an Chats oder das Herunterladen einer App „in Ordnung“ ist. Zu erreichen wäre dies z.B. durch einen Eltern-Account, welcher ebenfalls in dieser Anwendung verifiziert ist. Mögliche Optionen in dem Zusammenhang wären z.B. das Post-Ident-Verfahren, das Hinterlegen des Personalausweises oder ein Videoanruf zur Feststellung, ob eine erwachsene Person die Teilnahme bestätigt.

App-Schutzmechanismen für Minderjährige

Um Apps zu installieren oder so genannte In-App-Käufe zu tätigen, benötigen Kinder und Jugendliche mit einem Smartphone ein Konto bei Google oder Apple. Als zusätzlicher Schutz wäre ein Mechanismus denkbar, bei dem die Eltern eine Push-Benachrichtigung auf das Elternkonto erhalten. So könnten sie ihre Erlaubnis der Installation geben oder wenigstens die Information erhalten, dass sich ihre Kinder eine entsprechende App heruntergeladen haben. Da die jungen Opfer von potenziellen Täterinnen und Tätern nach erfolgter Anbahnung in einem Chat häufig zu einem Plattformwechsel getrieben werden, würden die Eltern bei dem Versuch eine neue App zu installieren eine Push-Benachrichtigung auf ihre Smartphones erhalten, um so rechtzeitig intervenieren bzw. die Situation prüfen und begleiten zu können. Wichtig ist, dass es hier lediglich um die Information für Eltern geht, welche Apps die Kinder (neu) nutzen wollen. Einige Unternehmen haben derartige Schutzmechanismen für App-Käufe und Downloads bereits erfolgreich implementiert. Entscheidend ist, dass diese Möglichkeiten auch bei den Eltern bekannter gemacht werden.

Reform des Netzwerkdurchsetzungsgesetzes (NetzDG)

Cybergrooming bezeichnet die Suche von Täterinnen und Tätern nach Opfern im Internet. Auf beliebten Plattformen oder in Videospielen verwickeln sie Kinder und Jugendliche in zunächst harmlose Gespräche, um sie später dazu zu drängen, Bilder und Videos zu schicken oder gar ein Treffen zu verabreden. Das NetzDG beinhaltet u.a. eine gesetzliche Berichtspflicht für Anbieterinnen und Anbieter sozialer Netzwerke über den Umgang mit Hasskriminalität und anderen strafbaren Inhalten, darunter auch

sexuelle Belästigung. Verstöße gegen diese Pflichten können mit Bußgeldern gegen das Unternehmen und die Aufsichtspflichtigen geahndet werden. Nicht erfasst von der Berichtspflicht sind allerdings Anbieter sozialer Netzwerke, die im Inland weniger als zwei Millionen registrierte Nutzer haben. Zahlreiche Anbahnungsversuche einer Straftat finden jedoch über kleinere Netzwerke, wie z.B. Knuddels, statt. Damit auch diese Netzwerke vom NetzDG erfasst und auch in ihrer Entstehung bereits mit der Thematik konfrontiert werden, sollte die Zahl der registrierten Nutzer z.B. auf 10.000 heruntergesetzt werden. Damit würden sie auch frühzeitig auf dem „behördlichen Radar“ auftauchen.

Darüber hinaus sind Messengerdienste vom NetzDG nicht erfasst. Diese erlauben aber im Einzelfall Gruppengrößen von bis zu 200.000 Nutzern und haben dann eine vergleichbare Reichweite wie soziale Netzwerke. Sie sollten deshalb ebenfalls vom Anwendungsbereich des NetzDG umfasst sein. Entscheidend ist dabei, dass Einzelchats und kleine Gruppen weiterhin vertraulich sind. Ebenfalls erfasst sein sollten Dienste für spezifische Inhalte, wie Plattformen für Pornografie, auf denen sich Missbrauchsdarstellungen von Kindern und Jugendlichen finden können. Solche Fälle müssen meldepflichtig werden.