VERBAND DER INTERNETWIRTSCHAFT E.V.

STELLUNGNAHME

zum Referentenentwurf eines Gesetzes zur Bekämpfung sexualisierter Gewalt gegen Kinder

Berlin/Köln 14. September 2020

Am 31. August 2020 hat das Bundesministerium der Justiz und für Verbraucherschutz (BMJV) einen Gesetzesentwurf zur Bekämpfung sexualisierter Gewalt gegen Kinder veröffentlicht und zur Diskussion gestellt. Mit dem vorliegenden Entwurf soll der Schutz von Kindern vor sexualisierter Gewalt durch ein ganzheitliches Konzept verbessert werden. Im Folgenden nimmt eco – Verband der Internetwirtschaft e.V. (eco) zu den Bereichen des Gesetzentwurfs Stellung, die für den Verband oder seine Mitglieder Relevanz haben.

eco unterstützt prinzipiell das Anliegen, sexualisierte Gewalt gegen Kinder umfassend zu bekämpfen. In diesem Sinne engagieren sich eco und seine Mitgliedsunternehmen seit rund 25 Jahren durch die Aktivitäten der eco Beschwerdestelle aktiv und erfolgreich gegen rechtswidrige Internetinhalte. Dabei liegt ein Fokus auf der Bekämpfung von Darstellungen des sexuellen Missbrauchs und der sexuellen Ausbeutung von Kindern und Jugendlichen.

Die Bekämpfung sexualisierter Gewalt gegen Kinder im Rahmen eines ganzheitlichen Konzepts ist dabei auch aus Sicht des eco essenziell. So kann einer Zerklüftung entgegengewirkt werden. Dies wiederum ermöglicht eine gute „Compliance“.

eco regt an, staatlicherseits im Sinne eines ganzheitlichen Konzepts auch Maßnahmen außerhalb von Gesetzesanpassungen in den Blick zu nehmen, um den begehrten Schutz zu erreichen, beispielsweise durch Aufklärungskampagnen und Förderung von Aktivitäten im Bereich der Bekämpfung der sexualisierten Gewalt gegen Kinder.

- Begrifflichkeitsanpassung

Durch die Entgegennahme und Bearbeitung von Hinweisen zu Darstellungen des sexuellen Missbrauchs und der sexuellen Ausbeutung von Kindern und Jugendlichen ist sich die eco Beschwerdestelle aus praktischer Erfahrung sehr bewusst, welchen Unrechtsgehalt derartige (Internet-)Inhalte und deren zugrundeliegende „Offline-Taten“ haben. eco begrüßt daher die vorgeschlagene Anpassung bei den im StGB verwendeten Begrifflichkeiten, könnte sich aber auch vorstellen, dass die Anpassung der Begrifflichkeiten noch weitergeht und auch Tatbestandsbezeichnungen der Kinder- und Jugendpornografie umfasst. Dies würde aus Sicht des eco auch hier den Unrechtsgehalt der Taten besser darstellen. Gleichzeitig könnte so ein Gleichklang auf internationaler Ebene bewirkt werden.

- Neufassung der §§ 176 ff. StGB

Im Hinblick auf die Neufassung der §§ 176 ff. StGB möchte eco anregen, die Formulierung der Versuchsstrafbarkeit bei sexualisierter Gewalt gegen Kinder ohne Körperkontakt und bei Grooming zu überdenken.

Denn durch § 176a StGB-E soll die sexualisierte Gewalt gegen Kinder ohne Körperkontakt mit dem Kind geregelt werden. Wesentliche Neuerung in diesem Deliktsfeld soll (neben der Strafrahmenanpassung) die Einführung der Strafbarkeit des untauglichen Versuchs in Bezug auf das Einwirken mit pornografischen Inhalten bzw. Reden sein. Künftig soll es auch strafbar sein, wenn der Täter nur annimmt, dass er auf ein Kind einwirkt, tatsächlich aber Kontakt zu einer erwachsenen Person besteht.

Die Intention des Gesetzgebers ist nachvollziehbar. Diesbezüglich schlägt eco jedoch vor, eine klare und einfach anwendbare Formulierung zu wählen, damit betroffene Diensteanbieter Sachverhalte einfach bewerten können, insbesondere bei zum Beispiel von Beschwerdestellen übermittelten Hinweisen zu verbotenen Inhalten oder im Rahmen von strafprozessualen Maßnahmen. Denn in der Praxis kann die aktuell gewählte Formulierung für Diensteanbieter zu Problemen führen. Für den Anbieter wird es regelmäßig schwer oder nicht nachvollziehbar sein, ob Person A irrig annimmt, dass Person B ein Kind ist.

Vorstellbar wäre zum Beispiel in diesem Bereich die Versuchsstrafbarkeit zu streichen und stattdessen in § 176a Abs. 1 Ziffer 3 zu ergänzen, dass dies auch beim Einwirken auf „Scheinkinder“ (Personen, die sich als Kind ausgeben) gilt. Das Ausgeben als Kind ist Anhand der (Fake-)Profildaten nachprüfbar.

Darüber hinaus stellt sich die Frage, ob die Regelung zum Einwirken mittels pornografischer Inhalte nicht womöglich im Rahmen des Grooming-Paragrafen (§ 176b StGB-E) stimmiger aufgehoben wäre, da diese Tathandlung üblicherweise Teil des Online-Groomings ist bzw. hiermit sehr eng im Zusammenhang steht.

Auch im Hinblick auf die Strafbarkeit des untauglichen Versuchs des Groomings regt eco eine Umformulierung analog zu den Anmerkungen zu § 176a StGB-E an.

- Anpassungen des Strafprozessrechts (§§ 100a, 100b, 100g StPO-E)

Der Gesetzentwurf sieht unter anderem vor, die Katalogtaten der Telekommunikationsüberwachung, der Onlinedurchsuchung sowie der Erhebung von Verkehrsdaten zu erweitern, um eine effektive Strafverfolgung im Bereich der sexualisierten Gewalt gegen Kinder und der Verbreitung, des Erwerbs und des Besitzes kinderpornographischer Inhalte zu ermöglichen.

eco teilt die Sichtweise, dass eine konsequente Strafverfolgung unverzichtbarer Teil der Bekämpfung sexualisierter Gewalt gegen Kinder (in all ihren Facetten) ist. Die eco Beschwerdestelle bringt daher grundsätzlich Hinweise zu Darstellungen des

sexuellen Missbrauchs Minderjähriger zur Anzeige und arbeitet dabei auch eng mit dem Bundeskriminalamt zusammen.

Durch die Neufassung der §§ 176 ff. StGB-E und die Strafrahmenanhebung der §§ 176 ff, 184b StGB-E kommt es zugleich zu einer Anpassung der Katalogtaten der Telekommunikationsüberwachung, der Onlinedurchsuchung sowie der Erhebung von Verkehrsdaten. Dies kann jedoch nicht über bestehende Probleme im Kontext dieser strafprozessualen Maßnahmen hinwegtäuschen.

Quellen-TKÜ und Online-Durchsuchungen bringen das Risiko mit sich, dass hierfür bestehende Sicherheitslücken ausgenutzt werden (könnten). Der entsprechende Anreiz für die Ermittlungsbehörden ist hoch. Die beiden technischen Ermittlungsinstrumente sind am einfachsten und besten zu nutzen, wenn sie durch Lücken in handelsüblicher und weit verbreiteter Software auf dem System des betroffenen Nutzers genutzt werden. Dann müssten die Ermittlungsbehörden nicht erst aufwendig nach einer Lücke auf dem IT- System des Verdächtigen suchen. Zudem erhöht ein solches Lückensuchen mit individuell zugeschnittener Software bzgl. des konkreten IT-Systems die Gefahr, dass der Zweck der Online-Durchsuchung eher vereitelt wird als bei bekannten, weitverbreiteten Softwarelücken. Denn es besteht eine hohe Wahrscheinlichkeit, dass das Lückensuchen mit individuell zugeschnittener Software dem betroffenen Nutzer auffällt (zum Beispiel durch ein geändertes Systemverhalten). Die bekannten, weitverbreiteten Lücken bergen dieses Risiko weniger, denn sie wurden zumeist vielfach erprobt, sei es durch Geheimdienste oder Cyberkriminelle. Bei einem hohen Entdeckungsrisiko, wären die Lücken entweder bereits geschlossen worden oder sie würden nicht genutzt, denn man will eben nicht entdeckt werden.

Sicherheitslücken können jedoch nicht nur deutsche Behörden nutzen, sondern auch Kriminelle und ausländische Geheimdienste. Eine Lücke, bspw. in Betriebssystemen zu Gunsten von Ermittlungen gegen eine Person offen zu halten, bedeutet für Millionen von privaten und gewerblichen Nutzern hierzulande Gefahren für deren Privatsphäre, deren Eigentum, mittelbar auch deren Vermögen. Zudem schafft das Offenlassen von Lücken die Gefahr, dass über diese Lücke Botnetze aufgebaut werden. Damit setzt man erhebliches Risiko für IT-Systeme landesweit und über die eigenen Grenzen hinaus, da Botnetze können sehr schnell wachsen können. Das Ausnutzen von Sicherheitslücken und deren Offenlassen gefährdet das Vertrauen und die Integrität und setzt Wirtschaft, Bevölkerung und auch den Staat einem Sicherheitsrisiko aus. Zudem stellen sich Haftungsfragen bei staatlichen angeordneten Eingriffen, bei denen Unternehmen zum Mitwirken gezwungen wurden.

Sofern in diesem Bereich Sicherheitslücken ausgenutzt werden, hält eco daher Quellen-TKÜ und Online-Durchsuchung für falsch und lehnt diese ausdrücklich ab. Denn festgestellte Schwachstellen sind aus Sicht des eco unverzüglich den Herstellern zu melden und zu schließen. Das Offenhalten von Sicherheitslücken gefährdet die gesamte Sicherheit und Integrität von IT-Systemen sowie die Privatsphäre aller Nutzer.

Im Hinblick auf den Einsatz von Staatstrojanern gilt es sicherzustellen, dass deren Fähigkeiten bzw. Reichweite beim Durchsuchen informationstechnischer Systeme kontrolliert werden kann. Das hierzu erforderliche technische Expertenwissen muss bei den Ermittlungsbehörden und Gerichten vorhanden sein und regelmäßig fortentwickelt werden.

Ganz grundsätzlich möchte eco an dieser Stelle auf die ausstehenden Entscheidungen des Bundesverfassungsgerichts zu Staatstrojanern und Vorratsdatenspeicherung hinweisen sowie auf die ständige Rechtsprechung des EuGH zur Vorratsdatenspeicherung und insbesondere auf das ausstehende Urteil zu C-520/18; Schlussantrag Rn. 113 – 118, 155. Nach Ansicht des eco ist es ratsam, diese Entscheidungen abzuwarten. Für einen Einklang zwischen StGB und StPO ist eine Anpassung der Straftatenkataloge in den §§ 100a, 100b, 100g StPO zwar angezeigt. Positiv bewertet wird daher aber auch, dass es keine weitergehenden „Verschärfungen“ an dieser Stelle gibt.
