



DIE BUNDESMINISTERIN
FÜR JUSTIZ

BMJ-Pr7000/0174-Pr 1/2010

XXIV. GP.-NR

5834 /AB

27. Aug. 2010

zu 5901 /J

An die

Frau Präsidentin des Nationalrates

Wien

zur Zahl 5901/J-NR/2010

Der Abgeordnete zum Nationalrat Mag. Johann Maier und GenossInnen haben an mich eine schriftliche Anfrage betreffend „Kinderpornographie im Internet – Löschen oder Web-Sperren (Access Blocking)?“ gerichtet.

Ich beantworte diese Anfrage wie folgt:

Zu 1:

Der Schutz vor sexueller Ausbeutung und sexuellem Missbrauch ist auch im internationalen Bereich ein zentrales Anliegen. Hierzu gehören etwa Maßnahmen zur Verhinderung der Herstellung und Verbreitung von kinderpornografischem Material. Erwähnenswert sind hierbei das Zusatzprotokoll zum Übereinkommen über die Rechte des Kindes betreffend Kinderhandel, Kinderprostitution und Kinderpornografie, die UN-Konvention über die Rechte des Kindes, das Übereinkommen des Europarates zum Schutz von Kindern vor sexueller Ausbeutung und sexuellem Missbrauch (CETS 201) sowie der Rahmenbeschluss des Rates zur Bekämpfung des sexuellen Missbrauchs und der sexuellen Ausbeutung sowie der Kinderpornografie. Der zuletzt erwähnte Rahmenbeschluss soll mit In-Kraft-Treten einer neuen Richtlinie des Europäischen Parlaments und des Rates zur Bekämpfung des sexuellen Missbrauchs und der sexuellen Ausbeutung von Kindern sowie der Kinderpornografie aufgehoben werden. Im Entwurf dieser Richtlinie werden die Mitgliedsstaaten verpflichtet, den bloßen Zugriff auf

Kinderpornografie unter Strafe zu stellen (in Österreich wurde eine solche Bestimmung mit dem zweiten Gewaltschutzgesetz eingeführt).

Zu 2 und 4 bis 7:

Diese Informationen stehen mir nicht zur Verfügung. Ich ersuche um Verständnis, dass ich im Rahmen des parlamentarischen Interpellationsrechts – im Hinblick auf den damit verbundenen unvermeidbar hohen Verwaltungsaufwand – keine rechtsvergleichenden Studien in Auftrag geben kann.

Zu 3:

Eine stets aktuelle Übersicht kann auf der offiziellen Website des Europarates unter

<http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=8&DF=02/06/2010&CL=GER>

abgerufen werden. Mir liegen keine Informationen darüber vor, wie weit jeweils die Umsetzung in diesen Staaten vorangeschritten ist.

Zu 8 bis 14 und 22 bis 25:

Diese Fragen fallen in den Wirkungsbereich der Frau Bundesministerin für Inneres, auf deren Beantwortung zur gleichlautenden Anfrage, Zl. 6900/J-NR/2010, ich verweisen darf.

Zu 15:

Im Ermittlungsverfahren stehen den Strafverfolgungsbehörden insbesondere die Ermittlungsmaßnahmen der Observation (§ 130 StPO), der verdeckten Ermittlung (§ 131 StPO), des Scheingeschäfts (§ 132 StPO) und der optischen und akustischen Überwachung von Personen (§ 136 StPO), jeweils unter den materiellen und formellen Voraussetzungen und unter Beachtung des Verhältnismäßigkeitsgrundsatzes, zur Verfügung. Das Strafprozessreformgesetz hat sich bewusst für eine technikneutrale Formulierung des Begriffs der „Überwachung von Nachrichten“ entschieden. Erfasst wird gemäß § 134 Z 3 StPO das Ermitteln des Inhalts von Nachrichten, die über ein Kommunikationsnetz (wie das Internet) iSv § 3 Z 11 TKG und mobile terrestrische Netze, Stromleitungssysteme, soweit sie zur Signalübertragung genutzt werden, Netze für Hörfunk und Fernsehen sowie Kabelrundfunknetze (Rundfunknetze), unabhängig von der Art der übertragenen Informationen, oder einen Dienst der Informationsgesellschaft iSv § 1 Abs. 1 Z 2 des

Notifikationsgesetzes ausgetauscht oder weitergeleitet werden. Neben den Kommunikationsinhalten bei der klassischen Sprachtelefonie kommen als Nachrichten und somit als Überwachungsobjekte iSd § 134 Z 3 StPO daher auch Inhalte von Funksprüchen, Telefaxen, Telex, E-Mails sowie Inhalte sogenannter „packed switched data“, wie z.B. SMS oder MMS in Frage. Da der Betreiber eines Chat-Forums als Host-Provider iSd. § 16 ECG anzusehen ist (vgl. u.a. MR 2006, 338), kann eine Überwachung von Nachrichten auf die zweite Alternative des § 134 Z 3 StPO iVm § 135 Abs. 3 StPO gestützt werden.

Eine „nicht öffentliche Kommunikation“ wie z.B. über ein lokales Netzwerk ohne Verbindung zu öffentlichen Netzen kann unter den Voraussetzungen der §§ 134 Z 4 iVm 136 StPO mittels einer optischen und akustischen Überwachung in Echtzeit verfolgt und überwacht werden. Da eine solche Kommunikation grundsätzlich nicht den Schutz des Fernmeldegeheimnisses genießt, wäre auch eine Sicherstellung der nicht öffentlichen Server nach § 110 StPO möglich (s. *Reindl-Krauskopf WK-StPO* § 134 Rz 43 bis 45). Sofern Nachrichten über öffentliche Kommunikationsdienste im Sinne des § 3 Z 3 TKG ausgetauscht werden, ist auch eine Überwachung von Nachrichten gemäß § 134 Z 3 iVm § 135 Z 3 StPO denkbar.

Zu 16:

Die Verpflichtung zur Löschung illegaler Inhalte, darunter auch Kinderpornografie, kommt nach den §§ 13 bis 17, insbesondere § 16 ECG, in Betracht. Die konkrete Durchführung der technischen Löschung kommt den Providern zu. Eine Entfernung bzw. Löschung von kinderpornographischem Material auf ausländischen Servern gehosteten Webseiten ist österreichischen Strafverfolgungsbehörden derzeit aus rechtlichen Gründen nicht möglich. Hier können die österreichischen Justizbehörden lediglich ein Rechtshilfeersuchen an jenen Staat richten, in dem sich ein Provider einer Webseite mit kinderpornographischem Inhalt befindet. Im Übrigen verweise ich auf die Beantwortung der Frau Bundesministerin für Inneres zur gleichlautenden Anfrage Zl. 6900/J-NR/2010.

Zu 17 und 19:

Aufgrund der dezentralen Struktur des Internets können zwar verbotene Inhalte nicht lückenlos gesperrt und Zugriffe auf solche Seiten nicht dauerhaft verhindert werden. Ich halte aber jede signifikante Erschwerung des Zugangs zu illegalen Webinhalten

für wichtig. Legislative Maßnahmen, wie etwa das Pönalisieren der Verbreitung und des Abrufens von einschlägigen Inhalten, entfalten eine präventive Wirkung auf die Normunterworfenen.

Durch das zweite Gewaltschutzgesetz – 2. GeSchG (BGBl. I Nr. 40/2009) wurde der Tatbestand des § 207a Abs. 3a StGB eingeführt, der mit 1. Juni 2009 in Kraft getreten ist. Nunmehr wird ein (bloß) wissentlicher Zugriff auf eine pornografische Darstellung Minderjähriger im Internet unter Strafe gestellt. Es sollen dadurch jene Fälle erfasst werden, in denen der Täter die Bilder nicht speichert (ansonsten wäre ein Besitz gegeben). Nach dem JAB (106 BlgNR XXIV. GP Seite 35) muss der Zugriff unmittelbar auf die pornografische Darstellung erfolgen, sei es, dass etwa schon eine geöffnete Startseite einer Homepage eine solche Darstellung enthält, sei es, dass ein Link zu einer solchen Darstellung geöffnet wird. Deshalb wurde im Bereich der Kinderpornographie der Schutzzweck des § 207a StGB entsprechend ausgeweitet, wodurch der Druck auf die „Konsumenten“ derartiger Bilder und daher mittelbar auch auf die (zumeist nicht oder schwer greifbaren) Anbieter erhöht werden sollte.

Auch Provider können sich nach § 207a Abs. 1 StGB (allenfalls in Verbindung mit § 3 VbVG) strafbar machen. Bei den Providern wird man grundsätzlich differenzieren müssen; jene Provider, die ganz allgemein einen Server betreiben, um anderen Personen einen pauschalen Zugang zum Internet zu eröffnen, werden – mangels Konkretisierung der Tat und des Tatvorsatzes – nicht schon allein aufgrund des allgemeinen Zugänglichmachens von Kinderpornografie beteiligt sein (vgl. Auer/Loimer, Zur Strafbarkeit der Verbreitung von Kinderpornographie über das Internet, ÖJZ 1997, 618 ff; Kienapfel/Schmoller BT III § 207a Rz 18). Wer aber gespeicherte Abbildungen über das Internet bewusst (d.h. bei Kenntnis der gespeicherten Inhalte) an unbekannte Computerbenutzer weitergibt, macht sich strafbar nach § 207a Abs. 1 Z 3 StGB (vgl. Schick in WK-StGB² Rz 19 § 207a).

Auf europäischer Ebene wird derzeit ein Vorschlag für eine Richtlinie zur Bekämpfung von sexueller Ausbeutung von Kindern und Kinderpornografie verhandelt, der auch Bestimmungen zur Verpflichtung von Zugangssperren zu kinderpornografischen Inhalten im Internet umfasst. Die Verhandlungen sind noch nicht abgeschlossen. Vor dem Hintergrund des globalen Problems der

Kinderpornografie im Internet ist ein gemeinsames koordiniertes Vorgehen der EU-Mitgliedsstaaten erforderlich. Die Praxiserfahrungen jener Mitgliedsstaaten, die ein „access blocking“ entweder durch gesetzliche Regelung oder durch freiwillige Verpflichtung der Provider bereits durchführen, werden in den Verhandlungen berücksichtigt. Im Rahmen der Bekämpfung der Kinderpornographie im Internet ist für mich sowohl das Sperren von Webseiten mit kinderpornographischem Inhalt als auch das Löschen kinderpornographischer Inhalte vorstellbar.

Zu 18:

Alle verhältnismäßigen Maßnahmen sollten ergriffen werden, um die Verbreitung kinderpornographischer Inhalte zurückzudrängen und womöglich zu verhindern. Es wird vom Bundeskriminalamt laufend versucht, kinderpornographisches Material aus dem Netz entfernen bzw. löschen zu lassen. Aufgrund technischer und rechtlicher Gegebenheiten ist dies jedoch nicht immer möglich und sollte in diesen Fällen durch eine Sperre der Webseite ein weiteres Verbreiten verhindert werden. Wie bereits zu Frage 16 dargestellt kann die Löschung kinderpornographischer Inhalte bei auf ausländischen Servern gehosteten Internetseiten derzeit nur im Wege eines Rechtshilfeersuchens erfolgen. So gesehen kann eine Internetsperre insbesondere in diesem Bereich eine sinnvolle Ergänzung zu den Bemühungen des Löschens kinderpornographischer Inhalte darstellen.

Zu 20 und 21:

Die internationale Zusammenarbeit zwischen den Strafverfolgungsbehörden gestaltete sich im Allgemeinen problemlos. Zur Durchführung eines Strafverfahrens nach § 207a StGB gegen einen inländischen Betreiber oder Täter bedarf es in der Regel keiner Rechtshilfeersuchen, weil in der überwiegenden Zahl der Fälle durch entsprechende Provider- und Verbindungsdaten hinreichende Beweise vorliegen.

Bei Verdacht der Verbreitung oder Bereithaltung von kinderpornografischem Material auf oder durch ausländische Server setzt die Meldestelle für Kinderpornografie beim Bundeskriminalamt die ausländischen Sicherheitsbehörden immer über diesen Sachverhalt in Kenntnis. Damit werden auch Fälle abgedeckt, bei denen eine Zuständigkeit der österreichischen Justizbehörden nicht besteht.

Statistiken über die Löschung ausländischer Websites mit kinderpornografischem Inhalt werden im Bundesministerium für Justiz nicht geführt.

Zu 26 und 27:

Solche Statistiken werden im Bereich des Bundesministeriums für Justiz nicht geführt.

Zu 28:

Eine Löschung oder Entfernung von Websites oder Inhalten auf Servern in anderen Mitgliedsstaaten der EU ist den österreichischen Justizbehörden nicht möglich.

Nach § 59a des Auslieferungs- und Rechtshilfegesetzes (ARHG) und Art. 7 des Übereinkommens zwischen den Mitgliedsstaaten der Europäischen Union vom 12. Juli 2000, BGBl. III Nr.65/2005, können die Gerichte und Staatsanwaltschaften Informationen über Server, auf denen sich kinderpornografisches Material befindet, den zuständigen Behörden des anderen Mitgliedsstaates zur Einleitung und Durchführung eines Strafverfahrens übermitteln.

Sollten Missstände in einem Mitgliedsstaat bei der Anwendung von Artikel 3 des Rahmenbeschlusses 2004/68/JI des Rates vom 22. Dezember 2003 zur Bekämpfung der sexuellen Ausbeutung von Kindern und der Kinderpornografie bestehen und der Vertrieb, die Verbreitung und die Weitergabe von Kinderpornografie unter Verwendung eines EDV-Systems nicht bekämpft werden, kann in sinngemäßer Anwendung von Artikel 12 dieses Rahmenbeschlusses der Rat unterrichtet werden.

Zu 29:

Neben den bereits zu Frage 15 erwähnten Maßnahmen könnten bestimmte Filtermethoden sowie die Umsetzung der Richtlinie 2006/24/EG über die Vorratsdatenspeicherung Unterstützung im Kampf gegen Kinderpornografie bieten.

Zu 30 und 31:

Solche Statistiken werden im Bereich des Bundesministeriums für Justiz nicht geführt.

Zu 32:

Ich verweise auf die Beantwortung der Frage 28.

Die Übereinkommen des Europarats über Computerkriminalität (CETS 195) und zum Schutz von Kindern vor sexueller Ausbeutung und Missbrauch (CETS 201) enthalten

Konsultations- und Überwachungsbestimmungen, die die problemlose Anwendung in allen Mitgliedsstaaten sicherstellen sollen.

Zu 33 und 34:

Nach den dem Bundesministerium für Justiz vorliegenden Informationen wenden Schweden, Finnland, Dänemark, Großbritannien (mit Nordirland), die Niederlande und Spanien das Webfiltering (Verhinderung des Zugriffs auf kinderpornografische Webseiten) an. Frankreich, Tschechien und Italien bereiten die Einführung dieser Maßnahme vor. Neben den EU-Mitgliedsstaaten wenden Norwegen und die Schweiz das Webfiltering an.

Dem Bundesministerium für Justiz liegen keine Informationen darüber vor, ob und für welche weiteren strafbaren Handlungen (neben der Verbreitung von kinderpornografischem Material) in diesen Ländern Webfiltering betrieben wird.

Zu 35 und 36:

Bisher liegen keine Studien über die Auswirkungen dieser Maßnahmen in den genannten Ländern vor. Erfahrungsberichte aus Ländern, die Webfiltering praktizieren, waren positiv.

Zur Frage der Umgehung verweise ich auf meine Antwort zur Frage 19.

Zu 37:

Die Initiative Stopleveline ist eine wichtige Stütze im Kampf gegen die Verbreitung von Kinderpornografie im Internet. Ich halte den Informations- und Meinungsaustausch in diesem Beirat, dem neben Vertretern des Bundesministeriums für Justiz und des Bundesministeriums für Inneres (Meldestelle) auch Vertreter der Provider und der Wissenschaft sowie andere Internet-Experten angehören, für positiv. Die Zusammenarbeit der österreichischen Initiative mit Partnerorganisationen im Rahmen der europäischen Initiative INHOPE wird als effizient beurteilt.

Zu 38:

Meinen Informationen zufolge wird ein eigenverantwortliches Filtern von illegalen Inhalten seitens der Provider in Österreich nicht in Aussicht gestellt. Die Gründe dafür sind mir nicht bekannt.

Zu 39:

Die Tätigkeit nationaler oder internationaler freiwilliger Meldestellen wie z.B. Stopline oder INHOPE bewerte ich als wichtigen Beitrag im Kampf gegen kinderpornografisches Material im Internet. Eine weitere Verstärkung der internationalen Zusammenarbeit der freiwilligen Beschwerdestellen auch im außereuropäischen Raum würde ich sehr begrüßen.

Zu 40:

Die Frage einer Beteiligung Österreichs an der „Financial Coalition“ betrifft den Zuständigkeitsbereich des Bundesministeriums für Inneres.

Zu 41 und 42:

Im Oktober 2009 haben die Justiz- und Innenminister eine Schlussfolgerung auf der Tagung des Europäischen Rates verabschiedet, in der der im März 2009 erfolgte Start der Europäischen Finanzkoalition (EFK) begrüßt wird. Für deren Aktivitäten gegen den sexuellen Missbrauch im Internet will die Europäische Kommission bis zu 427.000 Euro bereitstellen. Weiters fordert der Rat die Mitgliedsstaaten auf, dieser von MasterCard, Microsoft, PayPal, VISA Europe und der zivilgesellschaftlichen Organisation Missing Children Europe gegründeten "European Financial Coalition" beizutreten. Die EU-Länder sollen den Aufbau eigener nationaler Finanzkoalitionen gegen die Verbreitung von Kinderpornografie im Netz befördern. Im Rahmen solcher von Staat, Wirtschaft und Gesellschaft getriebener Ansätze sei sicherzustellen, dass Prozesse zur Opferidentifizierung Vorrang genießen, entwickelt und ausformuliert werden. Weiteres Ziel müsse die Implementierung eines Kontrollsystems mit Unterstützung aller an Internet-Bezahlösungen beteiligter Parteien sein, um die kommerzielle Seite "dieses wachsenden Geschäfts" zu behindern. In die Netzwerke einbezogen werden sollen klassische Finanzdienstleister sowie Internet- und E-Mail-Anbieter. Diesen legt der Rat nahe, Organisationsverfahren und geeignete Zusätze zu ihren Geschäftsbedingungen zu entwickeln, um Straftäter zu isolieren und der Verbraucherseite Steine in den Weg zu legen. Im Rahmen dieser Finanzkoalitionen soll die Zusammenarbeit zwischen den Wirtschaftspartnern und Sicherheitsbehörden ausgebaut werden. Dafür sei nach dem Inhalt der Schlussfolgerung ein Kooperationsmodell zu entwickeln. „Aufklärungsinformationen und operationale Einsichten“ in die „Natur des Verhaltens von Straftätern“ sollen der Finanzindustrie

helfen, das Problem mit aller Macht anzugehen. Schließlich wünscht der Rat Studien und Analysen zur Beleuchtung des Phänomens unter besonderer Berücksichtigung sich entwickelnder neuer Bezahlmethoden. Auch die Kommission wird aufgefordert, entsprechende Untersuchungen zu erleichtern und über die Fortschritte der EFK zu berichten.

Ein Endbericht über das Projekt liegt derzeit noch nicht vor, weshalb Umsetzungsüberlegungen verfrüht wären. Grundsätzlich wird aber eine Überwachung von Online-Bezahlsystemen zur Bekämpfung des Konsums von kinderpornographischen Inhalten für sinnvoll erachtet.

Zu 43:

Diese Frage lässt sich mit dem Datenmaterial der Verfahrensautomation Justiz nicht beantworten; es wären somit bundesweite händische Recherchen aller Fälle, in denen ein Sachverhalt nach § 207a StGB vorgelegen ist, erforderlich. Im Hinblick auf den damit verbundenen unvertretbar hohen Verwaltungsaufwand ersuche ich um Verständnis, wenn ich von einem derartigen Berichtsauftrag an die Staatsanwaltschaften abgesehen habe.

Aus den Sicherheitsberichten für die Jahre 2005 bis 2008 (für das Jahr 2009 liegen mir noch keine Zahlen vor) ergibt sich, dass in diesen vier Jahren insgesamt 1.948 Fälle angezeigt und 653 Personen verurteilt wurden.

26. August 2010



(Mag. Claudia Bandion-Ortner)