An das
Bundesministerium für Justiz
per E-Mail

Wien, am 23. Februar 2009

Betreff: Entwurf für eine Strafbestimmung betreffend Zugriff auf pornografische Darstellungen Minderjähriger im Internet

Sehr geehrte Damen und Herren!

Der Kampf gegen Kinderpornografie und andere illegale Inhalte im Internet hat für die ISPA und ihre Mitgliedsunternehmen sei Jahren höchste Priorität. Die Zusammenarbeit und Kooperation mit dem Bundeskriminalamt, den Strafverfolgungsbehörden sowie der Betrieb der nationalen Meldestelle Stopline und deren Einbindung in das internationale Netzwerk von Beschwerdestellen (INHOPE) leisten bereits heute einen wesentlichen Beitrag zur Bekämpfung der Kinderpornografie sowie zu einer erfolgreichen Ermittlung und Strafverfolgung der Täter.

Die ISPA erlaubt sich, zum Entwurf für einen neuen § 207a Abs 3a StGB in Bezug auf den Zugriff auf pornografische Darstellungen Minderjähriger im Internet folgende Stellungnahme abzugeben:

Nach Durchsicht der Vorlage inklusive Erläuterungen ist nach unserer Auffassung die geplante Aufnahme des „wissentlichen Zugriffs auf eine pornografische Darstellung Minderjähriger“ in den Straftatbestand aus folgenden Gründen problematisch.

1. **Begriffliche und technische Probleme im Zusammenhang mit dem Begriff „wissentlicher Zugriff“**

1.1. Fehlende Schärfe in der begrifflichen Bestimmung

Der in das StGB neu aufzunehmende Absatz des § 207 a (3a) besagt:

> Nach Abs.3 wird auch bestraft, wer im Internet wissentlich auf eine pornografische Darstellung Minderjähriger zugreift.

Damit soll in Hinkunft nicht nur die auf Besitz ausgerichtete Verschaffenshandlung einschlägiger Darstellungen strafbar sein, sondern auch das bloße Betrachten (der „Konsum“). Derzeit fällt erst die Abspeicherung eines zunächst nur im Arbeitsspeicher des Datenverarbeitungsgeräts vorhandene bildliche Darstellung auf einem Speichermedium unter den Tatbestand des Abs 3.

Zunächst fällt auf, dass bereits der Begriff des „Zugreifens“ nicht näher ausgeführt ist. Im Gegensatz zum Besitz einer pornografischen Darstellung Minderjähriger, bei dem die Abbildungen am Datenverarbeitungsgeräts des Täters abgespeichert sind

address: 1090 wien, währingerstraße 3/18 • austria • europe
phone: +43-1-4095576 • fax: +43-1-409557621 • mail: office@ispa.at • web: http://www.ispa.at • zvr:551223675
UID-Nr.: ATU 543 97 807 • IBAN=AT59 1200 0006 6049 1705 • BIC=BKAUATWW • blz:12000 • bank austria:00660491705 • dvr:0931977

und so leicht einer Verifikation unterzogen werden können, ist der Beweis, dass ein Benutzer bzw Täter auf derartige Inhalte nur „zugegriffen“ hat jedoch tatsächlich aus mehreren Gründen (siehe unten) schwierig zu führen.

Des Weiteren betont der Gesetzgeber, dass der Zugriff gem. § 5 Abs. 3 StGB „wissentlich“ erfolgen muss, d.h. dass der Täter den Umstand, dass er auf eine pornografische Darstellung Minderjähriger nach § 207a Abs. 4 zugreift, nicht bloß für möglich, sondern für gewiss halten muss.

Es wird vom Gesetzgeber aber nicht genau ausgeführt, was im Detail der im Zusammenhang mit „wissentlich“ erwähnte „wiederholte Zugriff“ auf einschlägige Inhalte bedeutet. Dies erscheint jedoch vor allem wegen der unten angeführten technischen Merkmale des Internet-Datenverkehrs im Hinblick auf eine potenziell erfolgreiche Beweisführung unumgänglich zu sein.

Die technischen Probleme stellen sich wie folgt dar:

1.2. Der Datei- bzw Linkname entspricht nicht dem Datei- bzw Linkinhalt

Da beim Tatbestand des vorgeschlagenen § 207a Abs. 3a per definitionem kein Besitz notwendig ist, d.h. keine Kopie der pornografischen Darstellung Minderjähriger auf dem Datenverarbeitungsgerät oder einem Speichermedium des Benutzers gespeichert ist, muss bei der Beweisführung im Bezug auf eine Straftat entweder auf eine Dateibezeichnung oder einen Link, d.h. den aufgerufenen URL (Uniform Resource Locator), zurückgegriffen werden.

Dies ist aus mehreren Gründen problematisch. Allgemein gilt, dass der Name einer Datei völlig unabhängig von dem jeweiligen Dateiinhalt gewählt werden kann. Dies bedeutet, dass pornografische Darstellungen Minderjähriger einen absolut unverfänglichen Dateinamen haben können. Es ist damit sehr leicht durch die Namensgebung nicht-problematische Inhalte „vorzutäuschen“. Für Internetadressen, wie sie beispielsweise in den Verlaufsdaten eines Internet-Browsers gespeichert werden können (auch diese Aufzeichnung kann vom erfahreneren Benutzer leicht ausgeschalten werden) heißt das, dass diese neben der Adresskomponente (Domain Namen/URL oder IP Adresse) ebenfalls eine im Hinblick auf Kinderpornografie unproblematische Dateibezeichnung tragen können. So könnte es sich zum Beispiel bei der (fiktiven!) Adresse http://133.34.54.21/pics/pezibaer.jpg um die Darstellung einer bei Kindern beliebten Bärenfigur, oder aber eine pornografische Darstellung Minderjähriger handeln. Dass Websites mit kinderpornografischen Inhalten sehr oft ihre Standorte wechseln, ist ein zusätzlicher Aspekt, der eine Überprüfung von Internetadressen auf deren tatsächlichen Inhalt ex post oft nicht zulässt. Dies wäre aber notwendig, da die einschlägige Darstellung nicht auf dem Datenverarbeitungsgerät des Benutzers gespeichert ist.

Weiters ist zu berücksichtigen, dass ein Link, der am Vortrag auf problematische Inhalte verwiesen hat, bereits am nächsten Tag völlig unbedenklich sein kann, da sich neben den oben beschriebenen technischen Komponenten die Inhaberschaft an einer dahinter stehenden Domain und somit der darauf publizierte Inhalt ändern kann. Der Zugriff auf dieselbe URL muss daher auch aus diesem Grund nicht denselben Inhalt zurückliefern.

address: 1090 wien, währingerstraße 3/18 • austria • europe
phone: +43-1-4095576 • fax: +43-1-409557621 • mail: office@ispa.at • web: http://www.ispa.at • zvr:551223675
UID-Nr.: ATU 543 97 807 • IBAN=AT59 1200 0006 6049 1705 • BIC=BKAUATWW • blz:12000 • bank austria:00660491705 • dvr:0931977

1.3. Dynamische Dateinamen bzw Links

Das oben beschriebene Problem der unverfänglichen Namensgebung wird bei jenen Websites noch verstärkt, die technisch dynamisch aufgebaut sind, und bei denen Inhalte ohne konkrete Namensbezeichnung aus einer Datenbank in auf den Webseiten dafür vorgesehenen Platzhalter geladen werden. Bei dieser Technik werden Dateinamen und Links dynamisch generiert, d.h. sie können einmalig sein und sich bei jeder Anfrage durch einen Webbrowser verändern, was eine ex post Überprüfung basierend auf Dateinamen bzw. Link-Adressen ebenfalls schwierig bis unmöglich gestaltet.

1.4. Abgesetzte Abfrage, jedoch keine Serverrückmeldung

Beim Aufruf einer bestimmten Internetadresse durch einen Webbrowser laufen auf einer bildhaften Ebene ähnliche Prozesse ab wie bei einem Telefonanruf. Hebt der korrespondiere Anrufpartner nicht ab, so kommt kein Gespräch zustande. Bezogen auf die Internettechnologie bedeutet dies, dass von einem Browser aufgerufene Inhalte nicht notwendiger Weise tatsächlich vom Server, auf dem sie gespeichert sind, übermittelt wurden (der Server „hebt nicht ab“). In solchen Fällen – wie sie bei Serverüberlastung oder schlechten Internetverbindungen entstehen können – kommt es möglicherweise zu keiner Darstellung der Inhalte, obwohl der Benutzer versucht hat (möglicherweise sogar wiederholt) darauf zuzugreifen. Ist in solchen Fällen trotz Nicht-Darstellung ein Zugriff erfolgt?

1.5. Abfragen durch Schadsoftware (nicht „wissentlich“ getätigte Abfragen)

Ein weiterer Punkt betrifft einen Aspekt der in Ziffer 6. der Erläuterungen (letzter Satz erster Absatz) angeführt ist:

> Nach wie vor nicht strafbar sein soll auch das Betrachten einer einschlägigen Darstellung auf einer von einer vom Betrachter verschiedenen Person und ohne dessen Zutun aufgerufenen Internetadresse sein.

Gerade Fälle der jüngsten Vergangenheit haben gezeigt, dass es nicht eine „vom Betrachter verschiedene Person“ sein muss, die einschlägige Darstellungen aufgerufen haben muss. Durch Schadsoftware (Würmer, Viren, Trojaner) kann es ebenfalls zu derartigen Aufrufen kommen, die in der Regel vom Benutzer oft erst spät bemerkt werden. Der Besitzer des Datenverarbeitungsgeräts hat in diesen Fällen möglicherweise schon auf hunderte einschlägige Darstellungen zugegriffen ohne je eine Darstellung tatsächlich gesehen zu haben. Auch nach Entfernung der Schadsoftware sind unter Umständen noch Aufzeichnungen über Aufrufe von pornografischen Darstellungen Minderjähriger vorhanden, obwohl die Schadsoftware, die sie aufgerufen oder abgefragt hat bereits deinstalliert werden konnte.

1.6. Grundproblem der technischen Umgehung

Um die technischen Ausführungen abschließend zu ergänzen weist die ISPA auf die für technisch versierte und erfahrene Benutzer anwendbare Möglichkeiten hin, die v.a. im Bereich von Peer-to-Peer einen anonymen Datenaustausch ermöglichen. Aufgrund dieser (und anderer alternativen) Techniken stellt der Abruf von pornografischen Darstellungen Minderjähriger über Webbrowser nur einen Teil der getauschten einschlägigen Inhalte dar.

address: 1090 wien, währingerstraße 3/18 • austria • europe
phone: +43-1-4095576 • fax: +43-1-409557621 • mail: office@ispa.at • web: http://www.ispa.at • zvr:551223675
UID-Nr.: ATU 543 97 807 • IBAN=AT59 1200 0006 6049 1705 • BIC=BKAUATWW • blz:12000 • bank austria:00660491705 • dvr:0931977

2. Rechtliche Grundlagen bezüglich einer Beauskunftung von „Zugriffsdaten“

Geht es darum grundsätzlich festzustellen, welcher Benutzer eine bestimmte Internetadresse zu einem bestimmten Zeitpunkt aufgerufen hat, so ist ein entsprechendes Auskunftsbegehren durch die Behörden an die Internet-Zugangsanbieter einzuleiten. Dies ist bereits heute basierend auf § 207a Abs 3 leg cit Praxis und natürlich ist einem entsprechenden Auskunftsbegehren der Behörden bei Vorliegen einer entsprechenden Rechtsgrundlage und Nennung der gesetzlichen Voraussetzungen Folge zu leisten.

Da (noch) keine Pflicht zur Datenspeicherung besteht ist jedoch zu betonen, dass beispielsweise eine Auskunft darüber, wem eine bestimmte dynamische IP-Adresse zugeordnet war, nur dann erteilt werden kann, wenn und solange die entsprechenden Verkehrsdaten vorhanden sind. Wir verweisen in diesem Zusammenhang auf die Löschungsverpflichtung des § 99 TKG 2003. Insbesondere kennt das österreichische Recht noch keine Verpflichtung der Speicherung von Verkehrsdaten auf Vorrat (sogenannte Data Retention). Die Vorratsdatenspeicherung ist überdies zur Bekämpfung von schweren Straftaten (zB Terrorismus, organisierte Kriminalität), die mit einer Freiheitsstrafe von drei Jahren und darüber bedroht sind, vorgesehen, wobei das von § 207a Abs. 3a betroffene Strafausmaß ein bis zwei Jahre beträgt. Dies würde bedeuten, dass die bei der Vorratsdatenspeicherung gespeicherten Daten bei der Verfolgung von § 207a Abs. 3a nicht zu verwenden wären.

3. Bedenken im Hinblick auf die Umsetzung der Richtlinie zur Vorratsdaten-speicherung

In Österreich steht die Umsetzung der europäischen Richtlinie zur Vorratsdaten-speicherung unmittelbar bevor.

Durch die Aufnahme der Strafbestimmung im Bezug auf den Konsum von pornografischen Darstellungen Minderjähriger in der vorliegenden Form zum jetzigen Zeitpunkt steht die Möglichkeit im Raum, den neuen § 207a Abs 3a dahingehend zu interpretieren, die Vorratsdatenspeicherung in einer die Aufbewahrung und damit den Aufbewahrungsaufwand maximierenden Weise umzusetzen. Grund dafür ist, dass die ohnehin technisch problematische Beweisführung (siehe oben) nur bei Speicherung von möglichst vielen Daten (z.B. zum Nachweis eines wiederholten Zugriffs) einen gewissen Erfolg zeigen kann.

Dies ist grundsätzlich zu hinterfragen, wird ja dabei auch der Eingriff in Grundrechte durch unverhältnismäßigen technischen Aufwand maximiert, ein Aspekt der von der ISPA 2007 in einem Positionspapier zur Vorratsdatenspeicherung aufgegriffen und umfassend diskutiert wurde.

4. Geringer Erfolg der Erweiterung von § 207a im Verhältnis zu den notwendigen Maßnahmen bezüglich der Beweisführung

Dementsprechend weist die ISPA darauf hin, dass aufgrund der technischen und rechtlichen Problematik in der Beweisführung neben den Unschärfen der verwendeten Begriffe auch besonderes Augenmerk auf das beschriebene Unverhältnis zwischen dem zu erreichenden Erfolges (der Nachweis eines strafbaren Konsums von pornografischen Darstellungen Minderjähriger gem. dem geplanten § 207a Abs 3a) und dem technischen Aufwand der Implementierung, dem Eingriff in Grundrechte, den

address: 1090 wien, währingerstraße 3/18 • austria • europe
phone: +43-1-4095576 • fax: +43-1-409557621 • mail: office@ispa.at • web: http://www.ispa.at • zvr:551223675
UID-Nr.: ATU 543 97 807 • IBAN=AT59 1200 0006 6049 1705 • BIC=BKAUATWW • blz:12000 • bank austria:00660491705 • dvr:0931977

Kosten des Betriebes und dem erforderlichen Eingriff in die Netzinfrastruktur des Internetproviders zu legen ist.

Eine Erweiterung auf den (wiederholten) Zugriff führt unserer Ansicht nach aufgrund mangelnder Unterscheidungsmöglichkeit nach dem tatsächlichen Vorsatz des potentiellen Täters entweder zu einer überbordenden Kontrolle oder zu einer faktischen Nutzlosigkeit der Regelung. Während im ersten Fall, wenn auf Verdacht jede IP Adresse, die auf einschlägigen Servern wiederholt auftritt untersucht und verfolgt wird und damit auch Unbeteiligte mit dem Stigma der Kinderpornografie konfrontiert werden, besteht im zweiten Fall die begründete Gefahr, dass wenn die Regelung in der Praxis für nicht tauglich bewertet wird, das Vertrauen in die Rechtssicherheit sinkt und die Norm in der Bedeutungslosigkeit verschwindet.

5. Ausreichen der bestehenden Normenstruktur

Es liegt natürlich nahe jede Form des Konsums von kinderpornografischem Material zu sanktionieren, um möglichen Triebtätern kein Betätigungspotential zu bieten. Diesem Ansatz ist zwar grundsätzlich zuzustimmen, es sind jedoch insbesondere in diesem Zusammenhang mehrere Gründe gegeben, die gegen eine Ausweitung des Straftatbestands sprechen.

Der Großteil der einschlägigen Tätigkeiten in diesem Gebiet spielt sich faktisch in geschlossenen Communities ab, in denen eine Mitgliedschaft nur dann gewährt wird, wenn selbst eigenes kinderpornografisches Material zu Verfügung gestellt wird. Diese Handlungen sind bereits vom geltenden Rechtsrahmen erfasst und können technisch einfacher nachgewiesen werden. Neben der faktischen und der technischen Komponente ist hier auch die rechtliche Situation klarer: Während bei der neuen Regelung nachgewiesen werden muss, dass vorsätzlich auf eine Website zugriffen wurde, auf der Kinderpornografie (zum gleichen Zeitpunkt) verfügbar war und aus den Umständen ohne jeden Zweifel (in dubio pro reo) ableitbar war, dass der Zugriff in der Gewissheit gesetzt wurde, auf der Website einschlägiges Material zu finden, kommt die bisherige Regelung mit dem einfachen dolus eventualis – die Verwirklichung ernstlich für möglich halten und sich mit ihr abfinden – aus.

6. Alternative: Intensivierung der Zusammenarbeit auf Basis bestehender Instrumente der Selbstregulierung

Aus Sicht der ISPA ist eine intensive Zusammenarbeit mit den Sicherheitsbehörden und die stetige Förderung von Medienkompetenz sowie das Anbieten von unbürokratischen Hilfestellungen im Hinblick auf die Eindämmung der Produktion und des Konsums von pornografischen Darstellung von Minderjährigen die effektivste Möglichkeit sexuelle Ausbeutung von Kindern sowie Kinderpornografie nachhaltig zu bekämpfen. So betreiben die ISPs wertvolle freiwillige Initiativen mit dem Ziel gegen Kinderpornografie vorzugehen, die sich bisher schon sehr gut bewährt haben.

In diesem Zusammenhang sei auf die eingangs erwähnte und von der ISPA betriebene Meldestelle im Internet „Stopline“ (www.stopline.at) verwiesen, an die sich ein Internetnutzer – auch anonym – wenden kann, wenn er im Internet auf Webseiten mit kinderpornografischen Inhalten stößt. Stopline kooperiert im Rahmen der internationalen Dachorganisation INHOPE (www.inhope.org) mit derzeit 34 Partnerorganisationen aus 30 Ländern weltweit. Das Netzwerk ermöglicht die

address: 1090 wien, währingerstraße 3/18 • austria • europe
phone: +43-1-4095576 • fax: +43-1-409557621 • mail: office@ispa.at • web: http://www.ispa.at • zvr:551223675
UID-Nr.: ATU 543 97 807 • IBAN=AT59 1200 0006 6049 1705 • BIC=BKAUATWW • blz:12000 • bank austria:00660491705 • dvr:0931977

Weiterleitung von Meldungen, um illegale Inhalte in deren Ursprungsland zu bekämpfen. Die effiziente internationale Zusammenarbeit der INHOPE-Hotlines hat in der Vergangenheit bereits vielfach zu großen Fahndungserfolgen insbesondere im Bereich der Bekämpfung der Kinderpornografie geführt.

Zusammenfassung

Die ISPA hegt große Bedenken hinsichtlich der Aufnahme des neuen § 207a Abs 3a in das StGB. Diese gründen sich v.a. auf die Schwierigkeit der Beweisführung sowohl im Bezug auf die oben ausgeführten technischen Eigenschaften des Internet-Datenverkehrs als auch auf das Unverhältnis zwischen dem Erfolg des Nachweises einer begangenen Straftat gem. § 207a Abs 3a und den dafür notwendigen technischen und rechtlichen Maßnahmen.

Die Verfolgung von Straftätern im Zusammenhang mit § 207a scheint uns durch den bereits praxiserprobten Abs 3 ausreichend unterstützt und wir empfehlen gem. Art. 20 Abs. 4 der Europaratskonvention einen Vorbehalt gegen die Kriminalisierungsverpflichtung gem. Art. 20 Abs. 1 lit. F einzulegen.

Die ISPA als Dachorganisation der Internetwirtschaft Österreichs unterstützt die Ausführungen in 4.2. der Erläuterungen voll und ganz, nämlich dass Österreich in der Bekämpfung der Kinderpornografie eine führende Rolle einnimmt. Dabei sollte jedoch nicht auf kaum anwendbare gesetzliche Bestimmungen gesetzt werden, sondern eine Forcierung und noch stärkere Verankerung von selbstregulierenden Instrumenten auf europäischer und internationaler Ebene stattfinden, um existierende soziokulturelle Lücken für Kriminelle im Bereich Kinderpornografie nach und nach endgültig zu schließen.

Mit freundlichen Grüßen,

ISPA Internet Service Providers Austria

Dr. Andreas Wildberger
Generalsekretär

Ergeht per E-Mail an:

- Bundesministerium für Justiz zHd Dr. Christian Manquet
  christian.manquet@bmj.gv.at

address: 1090 wien, währingerstraße 3/18 • austria • europe
phone: +43-1-4095576 • fax: +43-1-409557621 • mail: office@ispa.at • web: http://www.ispa.at • zvr:551223675
UID-Nr.: ATU 543 97 807 • IBAN=AT59 1200 0006 6049 1705 • BIC=BKAUATWW • blz:12000 • bank austria:00660491705 • dvr:0931977