

**Zeitschrift:** Reihe Kriminologie / Schweizerische Arbeitsgruppe für Kriminologie =  
Collection criminologie / Groupe suisse de travail de criminologie

**Herausgeber:** Schweizerische Arbeitsgruppe für Kriminologie

**Band:** 19 (2001)

**Artikel:** Internet : ein rechtsfreier Raum?

**Autor:** Niggli, M. A. / Schwarzenegger, Ch.

**DOI:** <https://doi.org/10.5169/seals-1051173>

### **Nutzungsbedingungen**

Die ETH-Bibliothek ist die Anbieterin der digitalisierten Zeitschriften auf E-Periodica. Sie besitzt keine Urheberrechte an den Zeitschriften und ist nicht verantwortlich für deren Inhalte. Die Rechte liegen in der Regel bei den Herausgebern beziehungsweise den externen Rechteinhabern. Das Veröffentlichen von Bildern in Print- und Online-Publikationen sowie auf Social Media-Kanälen oder Webseiten ist nur mit vorheriger Genehmigung der Rechteinhaber erlaubt. [Mehr erfahren](#)

### **Conditions d'utilisation**

L'ETH Library est le fournisseur des revues numérisées. Elle ne détient aucun droit d'auteur sur les revues et n'est pas responsable de leur contenu. En règle générale, les droits sont détenus par les éditeurs ou les détenteurs de droits externes. La reproduction d'images dans des publications imprimées ou en ligne ainsi que sur des canaux de médias sociaux ou des sites web n'est autorisée qu'avec l'accord préalable des détenteurs des droits. [En savoir plus](#)

### **Terms of use**

The ETH Library is the provider of the digitised journals. It does not own any copyrights to the journals and is not responsible for their content. The rights usually lie with the publishers or the external rights holders. Publishing images in print and online publications, as well as on social media channels or websites, is only permitted with the prior consent of the rights holders. [Find out more](#)

**Download PDF:** 03.02.2026

**ETH-Bibliothek Zürich, E-Periodica, <https://www.e-periodica.ch>**

**EIN GESPRÄCH ZWISCHEN  
M. A. NIGGLI UND CH. SCHWARZENEGGER**

**INTERNET – EIN RECHTSFREIER RAUM?**

**S:** Die weltweite Vernetzung durch das Internet hat die Allgemeinheit in den 90er Jahren derart schlagartig in eine neue Dimension der Kommunikation katapultiert, dass die rechtliche Erfassung dieser neuen Struktur ganz einfach nicht Schritt halten konnte. Das gilt selbstverständlich auch für das Strafrecht. Dennoch ist zu sagen, dass von Anfang an kein Unterschied zwischen Online-und Offline-Straftaten gemacht wurde. Einen rechtsfreien Raum gab es in diesem Sinne nie! Probleme gab und gibt es aber bei der konkreten Strafverfolgung von Internetdelikten, insbesondere wegen der technischen Schwierigkeiten bei der Ermittlung und der grenzüberschreitenden Natur dieser Delikte.

Ein Beispiel: Am 4. Mai 2000 verbreitete sich der berüchtigte «I love you»-Virus innert kürzester Zeit von einem Computer zum nächsten über alle Kontinente. Die durch die Datenbeschädigungen und Wiederinstandstellungsarbeiten verursachten Schäden werden von der Swiss Re auf rund \$ 2,3 Mia. geschätzt. «I love you» war das neuntgrößte Schadensereignis des Jahres 2000! Die relativ simple Auslösung und Verbreitung des Computer-Virus war höchstwahrscheinlich von einem jüngeren Filipino in Manila ausgegangen. Obschon er von den philippinischen Behörden gefasst werden konnte, musste das Strafverfahren gegen ihn eingestellt werden, weil es in diesem Land schlicht keinen Straftatbestand gibt, der das Verbreiten von Computer-Viren oder die Datenbeschädigung unter Strafe stellen würde. Seine Straftaten unterstehen allerdings auch der schweizerischen Strafgewalt, weil sie auch in der Schweiz «erfolgreich» waren, d.h. zu massiven Schäden geführt haben. Sollte er sich einmal hier-

her begeben, könnte er also festgenommen und vor Strafgericht gestellt werden.

Das Internet wird faktisch zum rechtsfreien Raum, wenn ein Verhalten in einem Land strafbar, aber im Nachbarland legal ist. Man denke an die vielen Online-Spielbankenbetreiber auf karibischen Inseln, gegen die kaum etwas zu machen ist, weil ihre Angebote in diesen Ländern völlig legal sind.

**N:** Neben der vieldiskutierten Verbreitung von Kinderpornographie und rassistischen Inhalten gibt es noch eine Reihe anderer Kriminalitätsformen, für welche sich die internationalen Computernetze wegen der weiträumigen Wirkungen und des relativ geringen Entdeckungsrisikos ausgezeichnet eignen: Denken Sie an das Hacking, an Computerbetrügereien, an den Datenklau oder gar Computersabotage. Im Frühjahr 2000 wurden zum Beispiel mehrere grössere Server von Yahoo, CNN, Ebay und anderen mit sogenannten Denial of Service Attacks lahmgelegt. Dabei handelt es sich im Grunde genommen um ein völlig legales Verhalten, nämlich schlichte Informationsabfragen an den Zielrechner. Nur, beim Denial of Service Attack wird gleichzeitig eine riesige Menge von Anfragen abgeschickt, die dann vom Zielrechner nicht mehr bewältigt werden kann. Ist das überhaupt strafbar?

Aber nicht nur die dogmatische Erfassung ist zum Teil fraglich, noch frappierender ist der Rückstand bei der Verfolgung von Internetstraftaten. In der Schweiz gab es lange keine Ansprechpartner bei der Polizei. Heute gibt es zwar eine Meldestelle bei der Bundespolizei, doch fehlen ihr weitgehend die Strafverfolgungskompetenzen. Dringend notwendig wäre daher die Schaffung eines zentralen Kompetenzzentrums für Cyberkriminalität auf Bundesebene, welches entsprechende Fachkenntnisse und die internationale Zusammenarbeit verstärken müsste.

**S:** Noch zu diesem «Denial-of-Service Attack», den Marcel Niggli angesprochen hat. Hier ist eine internationale Harmonisierung in Vorbereitung: der Europarat ist an der Ausarbeitung einer Cyber-Crime Convention.<sup>1</sup> Darin sollen eine Reihe materieller Strafnormen geschaffen werden, die von allen Signatarstaaten ins nationale Strafrecht zu übernehmen sind. Ein gewichtiger Block darunter sind die Computerdelikte. Vorgesehen ist u.a. auch eine Strafnorm gegen solche «Denial-of-Service Attacks», also das Abstürzenlassen eines Rechners durch eine Vielzahl von Abfragen.

**N:** Aber das Problem ist auch hier, muss man gleich anfügen, dass es sich um den Entwurf einer Konvention handelt, der sich auf Dinge richtet, von denen wir uns einig sind, dass sie inakzeptabel sind. Dabei geht's in erster Linie um Geld, das ist im Wesentlichen der Regelungsbereich: klassische Vermögenskriminalität, begangen mit den Mitteln der Elektronik.

Was Inhaltsdelikte betrifft, und das ist ganz typisch, so sieht diese Cyber-Crime Convention einen einzigen Tatbestand vor. Und der stellt so ungefähr das Einzige dar, auf das wir uns in Europa, geschweige denn in der Welt einigen können: die Kinderpornographie.

Und selbst dies ist auch nur deshalb möglich, weil wir uns in Europa einig sind, dass Kinderpornographie nicht akzeptabel ist, insbesondere weil wir uns halbwegs einig sind, was in etwa ein Kind sei. Aber wenn wir das genauer anschauen, dann erscheint es nicht ganz so einfach anzugeben, wann die Kindheit aufhört. Da bestehen sehr unterschiedliche Meinungen.

**S:** Es wurde eben die Internationalität angesprochen. Da stellt sich sofort die Frage: Kann man überhaupt solche Straftaten in der Schweiz verfolgen? Darüber besteht keine Einigkeit. Soll eine Verfolgung bei jedem im Inland wahrnehmbaren Internetdelikt möglich

---

<sup>1</sup> CONSEIL DE L'EUROPE, Projet de convention sur la cyber-criminalité (Version N° 27 rev.), 25 mai 2001. Abrufbar unter: <http://conventions.coe.int/treaty/fr/projets/cybercrime27.htm> (Stand: 27.01).



sein oder nur bei bestimmten, die einen sogenannten technischen Erfolg in der Schweiz haben? Die Diskussion darüber ist in vollem Gange, auch im Ausland. Sie ist aber noch keineswegs entschieden. In der Schweiz gilt wie in den meisten kontinentaleuropäischen Staat das Ubiquitätsprinzip, d.h. es wird einerseits dort angeknüpft, wo der Täter die Handlung ausführt, andererseits dort, wo der Erfolg oder die Wirkung dieser Handlung eintritt (Art. 7 StGB).

Bei der Bestimmung dieser Tatorte gibt es Interpretationsschwierigkeiten. Es wird z.B. bezüglich des Hacking (unbefugtes Eindringen in eine Datenverarbeitungsanlage, Art. 143<sup>bis</sup> StGB) die Meinung vertreten, die Tat könne nur dort verfolgt werden, wo der Hacker die Tat ausführe. Die Gegenmeinung sagt, die Tat sei auch da begangen, wo der Computer stehe, in welchen eingedrungen wird. Dies zeigt, dass wichtige Fragen des Strafanwendungsrechts im Bereiche der Internetkriminalität noch nicht gelöst sind.

Ich möchte nur noch eines hinzufügen: Man sagt immer, der Erfolg, die Wirkung, sei etwas sehr Zufälliges. Also, in Fällen wie dem «I love you»-Virus oder dem aktuellen «Naked Wife»-Virus, von welchen viele Computer in der Schweiz befallen wurden, stellt sich dann die Frage: Kann man den Täter, wenn er sich z.B. bei der Ausführung der Tat in Afrika befand, später in der Schweiz vor Gericht stellen? Kann man ihn dafür nach schweizerischem Strafrecht belangen, und falls ja, ist das nicht etwas sehr Zufälliges, etwas Willkürliches?

Auf der andern Seite kann man aber genausogut den Handlungsort in Frage stellen. Auch der Handlungsort ist zum Teil zufällig. Stellen Sie sich vor, ein Engländer geht in die Skiferien nach Scuol, wählt von dort mit seinem Computer das Internet an (Dial-Up-Verbindung per Modem) und begeht eine Straftat. Der Handlungsort wäre dann in der Schweiz. Die englischen Behörden könnten ihn dort, wo er wohnt, unter Umständen gar nicht belangen. Oder stellen Sie sich eine Hacker-Konferenz in Berlin vor. Da treffen sich Hacker aus der ganzen Welt in Berlin und dringen von dort aus z.B. unbefugt in den

Rechner des WEF ein. Dann wäre der Handlungsort in Berlin, auch wenn die Täter kurz darauf wieder in alle Himmelsrichtungen verschwinden. Oder denken Sie an die Internet-Cafés. Man kann heute überall auf der Welt in ein Internet-Café gehen und schnell eine Straftat online begehen. Der Handlungsort ist in solchen Fällen genauso zufällig.

**N:** Wir haben vor allem deshalb ein Problem, weil das Strafrecht auf internationale Sachverhalte einfach nicht ausgerichtet ist. Das war bis anhin einfach nicht so problematisch, weil der Hauptharst der Fälle deutlich in die eine oder andere Zuständigkeit fiel. Schwieriger wurde es indes schon immer, wenn ein Fall landesübergreifend war. Auslegungsprobleme gibt es nämlich nicht nur im Hinblick auf die Anknüpfung an die nationale Strafgewalt, was ja ein eigenes Problemfeld darstellt. Darüber hinaus ist im Kontext der Internetkriminalität nicht einmal der Gehalt der Strafnormen zweifelsfrei. Denken Sie an die Pornographie. Da besteht z.B. eine Tatvariante im «Zugänglichmachen». Das ist schon im Physischen ein sehr weiter Begriff! Fraglich ist etwa, ob etwas zugänglich gemacht ist, wenn es in einem Schrank liegt, der abgeschlossen ist, an dem aber der Schlüssel steckt. Muss ich den Schlüssel dann noch abziehen, damit der Inhalt meinen eigenen Kindern gegenüber nicht zugänglich gemacht ist? Ganz schwierig wird es in dem Augenblick, in dem Sie einen strafbaren Inhalt haben, der sich irgendwo auf dem Netz findet und damit an sich zugänglich ist. Wird dieser grundsätzlich schon zugängliche Inhalt dann z.B. über einen Link noch zugänglicher gemacht?

Selbstverständlich wird der Zugang durch einen Link erleichtert. Nur: Ein Erleichtern ist eben kein Zugänglichmachen und ein Zugänglichmachen eines bereits zugänglichen Inhalts erscheint eigenartig. Die Frage danach, ob ein Link ein Zugänglichmachen darstellt, ist eben deshalb bereits schwierig zu beantworten, weil der Tatbestand in seiner Formulierung schlicht nicht orientiert ist auf das Internet und Konstellationen, bei denen Inhalte, die irgendwo einge-

spiesen werden, global zugänglich sind. Das erscheint als das Hauptproblem. In unserem Denken orientieren wir uns nach wie vor am klassischen (man möchte sagen analogen) Bereich, in dem ein Wegnehmen eben bedeutet, dass derjenige, dem etwas weggenommen wird, das Weggenommene nicht mehr hat, weil das Objekt einmalig ist (oder höchstens ersetzbar, weil vertretbar). Jetzt kann es plötzlich beliebig vervielfältigt werden.<sup>2</sup> Die Information und ihre Struktur ist, was die Informationsdelikte zu etwas völlig anderem macht.

**S:** Die Lösung dieser Probleme bereitet auch Schwierigkeiten, weil das Strafrecht grundsätzlich nationalstaatlich orientiert ist. Für uns ist die Grundeinheit der Nationalstaat. Als «Containertheorie der Gesellschaft» charakterisiert dies der deutsche Soziologie ULRICH BECK in seinem Buch «Was ist Globalisierung?»<sup>3</sup> Im Referat von HARTMUT SEMKEN ist sehr deutlich geworden, dass das Internet und die darauf verfügbaren Dienste nicht in diese nationalstaatlichen Schachteln passen, sondern etwas Globales sind. Auf dieser Ebene gibt es aber keine entsprechenden Strafnormen und Durchsetzungsinstrumente, also geht man weiterhin nach den nationalen Strafrechtsordnungen vor. Und das führt im Bereich der Internetkriminalität dazu, dass Strafverfahren wegen der gleichen Tat in ganz verschiedenen Ländern möglich werden.

Was ist zu tun? Was kann sinnvollerweise überhaupt bewirkt werden? Ich muss noch einmal auf diese Cyber-Crime Convention zurückkommen, welche im materiellen und formellen Strafrecht eine gewisse internationale Vereinheitlichung bringen wird. Nicht in allen Bereichen allerdings, denn was kulturell umstritten ist, kann nicht über eine solche Konvention geregelt werden. Doch in den Bereichen, wo Einigkeit erzielt werden kann, erleichtert ein solches internationales Vertragswerk die Verfolgung grenzüberschreitender In-

---

2 Zum Problem der Reproduktion bereits sehr früh: W. BENJAMIN: Das Kunstwerk im Zeitalter seiner technischen Reproduzierbarkeit, – in: Gesammelte Schriften, Bd. I/2, 2. Aufl., Frankfurt a.M. 1978, 431ff.

3 U. BECK, Was ist Globalisierung? Irrtümer des Globalismus – Antworten auf Globalisierung, 3. Aufl., Frankfurt a.M. 1997, 49f.

ternetdelikte und führt zur Etablierung eines internationalen Standards. Auch die Frage nach der nationalen Strafgewalt wird entschärft, da sich die Strafverfolgungsbehörden der betroffenen Staaten untereinander informieren und jenen Staat, in dem sich der Täter aufhält, ersuchen können, die Strafverfolgung zu übernehmen. Dieser muss dann aktiv werden, weil die gleichen Strafbarkeitsvoraussetzungen auch dort gelten. Damit werden die Chancen einer effektiven Strafverfolgung erhöht.

**N:** Aber! Anzumerken ist, dass wenn üblicherweise die Rede aufs Internet kommt, auf dessen Gefahren und wie sehr das Internet das Propagieren und Verbreiten von Schweinereien ermögliche, dass in diesem Kontext fast immer zwei grosse Bereiche angesprochen werden: die Pornographie, spezifisch Kinderpornographie, und die Rassendiskriminierung. Eine derartige Orientierung aber ist viel zu eng. Der grösste Teil der Pornographie wird durch die Cyber-Crime Convention gar nicht erfasst und Rassendiskriminierung wird schon gar nicht angesprochen, und dies, obwohl wir in Europa sind und diesbezüglich untereinander einiger als andere Länder. Man sollte nicht immer nach Amerika zeigen und behaupten, eine Bekämpfung dieser Inhalte scheitere an den USA. Auch in Europa besteht der immer unterstellte Konsens keineswegs zweifelsfrei, weil wir auch hier eben durchaus unterschiedliche Wertungen treffen, die fraglichen Inhalte aber überall zugänglich sind.

Auf diesem Hintergrund könnten wir auch im Traditionellen stehen bleiben, also beim Prinzip, dass jeder für sich tut, was er für richtig hält. D.h. jedes nationale Strafrecht definiert ganz autonom, was es für strafbar hält. Dazu ist nur notwendig, dass man sich für zuständig erklärt, und dafür finden sich natürlich dogmatische Konstruktionen; Christian Schwarzenegger hat es ja eben angesprochen. Die Lösung bestünde mithin darin, dass sich die Schweiz für alles zuständig erklärt, was über das Internet in der Schweiz abgerufen werden kann (sei es nun aufgrund der Deliktsstruktur: alles, was hier abgerufen werden kann, hat hier einen Erfolg, oder – wohl sauberer – über das

Weltrechtsprinzip: die Schweiz deklariert, für welche Delikte sie sich zuständig erklärt, unabhängig vom Handlungs- oder Erfolgsort). Zweifelhaft bleibt dabei einzig, dass sich die Schweiz mit 7 Millionen Einwohnern im Verhältnis zu rund 6 Milliarden Weltbevölkerung damit wohl in eine etwas anmassende Position begibt. Leicht anmassend natürlich nur, wenn man an die Bedeutung der Schweiz denkt.

**S:** Einverstanden, aber die Sache ist nicht ganz so einfach. Schränkte man nämlich die Anknüpfungskriterien zu stark ein, etwa indem man sagen würde, alles, was im Ausland ins Internet gestellt werde, falle nicht unter die Schweizer Strafhohheit, dann würde man den Tätern die Rechtswahl im Strafrecht ermöglichen, was doch etwas aussergewöhnlich wäre. Wenn z.B. ein Schweizer Neonazi rassistische Parolen online verbreiten wollte, müsste er sich bloss in die USA oder in irgendein anderes Land begeben, wo das nicht strafbar ist, und könnte dort unbehelligt den rassistischen Inhalt auf einem Webserver zum Abruf bereitstellen. Würde er das gleiche in der Schweiz tun, unterstünde er der hiesigen Strafgewalt und würde wegen Verstoßes gegen die Antirassismuskriterien (Art. 261<sup>bis</sup> StGB) bestraft werden. Die Auswirkungen der Tat in der Schweiz (und anderswo) – namentlich die Verletzung der Menschenwürde der jüdischen Bevölkerung – sind aber in beiden Fällen identisch. Der deutsche Bundesgerichtshof in Strafsachen hatte unlängst zu entscheiden, ob ein Australier, der volksverhetzende Inhalte auf einem australischen Webserver bereitstellt, die unter anderem in Deutschland abgerufen werden können, auch der deutschen Strafhohheit unterstehe. Der BGH bejahte dies auf der Grundlage des Ubiquitätsprinzips (§ 9 Abs. 1 3. Alt. dStGB), weil die rassistischen Inhalte geeignet waren, den öffentlichen Frieden in Deutschland zu gefährden und dies als inländischer Erfolgseintritt zu werten sei.

**N:** Gut, jetzt kann man da sagen, da sind wir nicht ganz einer Meinung. Was Christian Schwarzenegger ausführt, ist natürlich, Sie haben es bereits bemerkt, bisher auch nicht anders gewesen. Ich kann selbstverständlich in die Vereinigten Staaten reisen und mich dort



rassendiskriminierend äussern, so viel ich will. Das stellt überhaupt kein Problem dar. Das ist völlig zulässig. Das tun ja auch manche Leute, z.T. auch berühmte Politiker in den Staaten. Und nie käme jemand auf die Idee zu sagen: «Dieser Niggli muss bestraft werden, denn er geht in die Staaten und hält sich an die dort geltenden Gesetze.» Wie aber, wenn das, was ich dort äussere, durch irgend jemanden in der Schweiz abgerufen würde. Nehmen wir an, jemand in der Schweiz ruft meine Äusserungen ab, stellt eine Verbindung her über Telefon zum Ort, wo ich an einer öffentlichen Veranstaltung spreche, und hört es mit. Handle ich dann in der Schweiz? Wäre ich hier strafbar? Niemals, meine Damen und Herren, niemals. Selbstverständlich nicht. Man könnte höchstens darüber nachdenken, ob derjenige strafbar würde, der das Ganze abrufte. Aber da sind wir ja wieder ganz zurückhaltend. Hinsichtlich einer Strafbarkeit der Nutzer sind wir ganz, ganz zurückhaltend. Solches muss man tun dürfen, lautet der einstimmige Kanon. Man darf alles Konsumieren. Man darf sogar Kinderpornographie konsumieren, meine Damen und Herren, man darf sie gegenwärtig sogar besitzen (das soll geändert werden), aber das reine Konsumieren, Anschauen, Zuhören oder Wahrnehmen, das wird auch in Zukunft kaum unter Strafe gestellt werden.

Man sollte sich darüber im Klaren sein, dass wir prinzipiell nicht beim Nutzer ansetzen, weil wir dies nicht tun möchten. In diesen Kontext gehört letztlich auch, was Bundesrätin METZLER kürzlich in ihrer Antwort auf die Motion Pfisterer<sup>4</sup> geäußert hat: Es sei problematisch, den Internet-Provider gänzlich von der Strafbarkeit auszunehmen und zwar mit der folgenden Begründung (Zitat): «Wir müssen uns bewusst sein, dass der Zugangsvermittler häufig den einzigen Anknüpfungspunkt darstellt um beispielsweise gegen Internet-Seiten mit rassistischen oder kinderpornographischen Inhalten vorzugehen.»<sup>5</sup>

---

4 [www.parlament.ch/afs/data/d/gesch/2000/d\\_gesch\\_20003714.htm](http://www.parlament.ch/afs/data/d/gesch/2000/d_gesch_20003714.htm) (Stand: 16.5.2001).

5 Stellungnahme zur Motion PFISTERER durch Frau Bundesrätin METZLER vom 6. März 2001; einzusehen unter: [www.parlament.ch/ab/frameset/d/s/4606/25965/d\\_s\\_4606\\_25965\\_26155.htm](http://www.parlament.ch/ab/frameset/d/s/4606/25965/d_s_4606_25965_26155.htm) oder aber: Amtliches Bulletin 2001, 28.

Übersetzt heisst das: Den Autor können wir nicht belangen, oder wir versuchen es nicht, oder es ist halt irgendwie schwierig. Den Provider aber, den können wir belangen, denn der sitzt (auch nicht wirklich, aber irgendwie) hier. Wenn Sie das in den traditionellen Bereich des Strafrechts übersetzen, dann sehen Sie, was es bedeutet. Es bedeutet nichts anderes, als dass wir einfach irgend jemanden in diesem Lande für irgend etwas strafbar werden lassen wollen. Und entsprechend lassen wir halt dann wirklich jemanden strafbar werden. Ob die Strafbarkeit über die Gehilfenschaft begründet wird (begründet werden kann) oder nicht, ist dabei gar nicht die zentrale Frage. Zentral ist nur, dass wir jemanden verantwortlich machen wollen (können). Es ist Ihnen möglicherweise bekannt, dass ich nicht unbedingt ein grosser Rassendiskriminierungs-Fan bin. Die Ablehnung von Rassendiskriminierung darf aber nicht dazu führen, dass wir einfach deshalb, weil wir bestimmte Rechtspositionen verfolgen, klassische Strafrechtsdogmatik über den Haufen werfen und behaupten: «Jetzt müssten wir da irgend eine Strafbarkeit begründen.» So geht es nach meinem Dafürhalten, d.h. genauer: nach unserem Dafürhalten (da sind wir uns wieder einig) nicht.

**S:** Damit ist jetzt die Access-Provider-Verantwortung angesprochen, aber ich möchte doch noch kurz Paroli bieten zu den Ausführungen bezüglich der Auslandstaten. Die Anknüpfungsregeln hängen eben auch vom Deliktstypus ab. Wenn der Gesetzgeber gewisse Straftatbestände als abstrakte Gefährdungsdelikte konzipiert, weil er den Rechtsgüterschutz immer weiter in das Vorfeld der Rechtsgutsverletzung verlegen will, dann ist der Erfolg dieser Tatbestände eben die Gefahr selbst und an diese muss angeknüpft werden. Es gab diese Diskussion auch schon früher, z.B. im Zusammenhang mit illegalen Piratensendern, die auf hoher See operierten. Eine Beschränkung der Strafhoheit müsste m.E. durch andere Massnahmen erzielt werden.

Wir müssen aber jetzt zur möglichen Strafbarkeit von Internet-Service-Providern (ISP) übergehen. Es ist schon im Referat von HART-



MUT SEMKEN angeklungen, dass die Strafverfolgungsbehörden häufig nur nach einem «nahe liegenden» Verantwortlichen Ausschau halten, der an der Verbreitung der inkriminierten Inhalte oder Informationen im Inland beteiligt ist. Als Ersatz für die Verfolgung der Hauptverantwortlichen werden die reinen Zugangsvermittler und Infrastrukturanbieter verantwortlich gehalten. Wir beide sind der Ansicht, dass dies nicht stimmen kann.

Auch der internationale Vergleich zeigt, dass die überwiegende Mehrheit der Staaten zu dieser Schlussfolgerung gelangt ist und eine entsprechende Einschränkung der Strafbarkeit von Providern vorgenommen hat. Dabei wird nach den unterschiedlichen Provider-Funktionen unterschieden. Der Trias der Content-Provider (Anbieter eigener Inhalte), Host-Provider (Anbieter, die Informationen Dritter auf ihrem Rechner bereitstellen) und Access-Provider (reine Zugangsvermittlung) entspricht eine abgestufte Verantwortlichkeitsregelung. Bezüglich der im Votum der Bundesrätin METZLER angesprochenen Access-Provider geht die internationale Tendenz ganz eindeutig dahin, sie von der Strafbarkeit für die Informationsübertragung auszunehmen. Es gibt auch nach dem geltenden Strafrecht gute Gründe, wieso das so sein muss.

**N:** Eben, unser Hauptanliegen wäre an sich, dass wir uns bemühen sollten, allgemein geltende und akzeptierte strafrechtsdogmatische Strukturen nicht einfach deshalb aufzuheben, weil es sich um Internet handelt. Vielmehr wäre zu überlegen, wie wir das Problem innerhalb dieser Strukturen regeln könnten. Wir können nicht einfach Grundprinzipien von Täterschaft und Teilnahme oder vom Deliktscharakter über Bord werfen alleine aufgrund unseres Strafbedürfnisses. D.h., an sich könnten wir das natürlich tun. Dann aber sind wir weg von einer halbwegs systematischen Regelung. Dessen sollte man sich schon bewusst sein. Ein derartiges Vorgehen hat ja z.B. im Bereich des Betäubungsmittelstrafrechtes dazu geführt, dass wir ein eigentliches Chaos haben. Ganz unabhängig davon, ob man Betäubungsmitteln gegenüber eher tolerant oder repressiv eingestellt ist,

darf man wohl feststellen, dass das Betäubungsmittelgesetz grundsätzliche, im übrigen Strafrecht anerkannte Kategorien einfach über den Haufen wirft. Das gilt hinsichtlich Täterschaft und Teilnahme, hinsichtlich Versuch und Vollendung, aber auch hinsichtlich der Konkurrenz. Wenn es nun um die eben erwähnten Internet-Service-Provider geht, dann sind wir uns vermutlich einig, dass das Strafrecht anwendbar ist, dass das Internet kein rechtsfreier Raum ist. Anwendbar ist mithin das Strafrecht, wie es eben gegenwärtig besteht. Und wenn dieses Strafrecht eine Lücke haben sollte, dann können wir eine solche Lücke natürlich schliessen. Wenn wir aber den reinen Zugangsvermittler strafbar werden lassen wollen, dann sind vergleichbare Beispiele im analogen Raum doch eher auf der seltsamen Seite.

**S:** Dazu habe ich vor kurzem einen Artikel in einer Gratiszeitung gefunden. Sein Titel lautet: «Die SBB toleriert Kiffer.»<sup>6</sup> Und da steht dann im Text, die Kondukteure und das Personal stellten ständig fest, dass da so ein süsslicher Geschmack in den Raucherabteilen herrsche. Es gebe auch Kunden der SBB, die sich darüber ärgerten, aber die SBB unternehme nichts dagegen. Denkt man über diesen Bericht etwas genauer nach, stellt man unweigerlich die Parallelität zu den Access-Providern fest: Auch die SBB ist ein Service-Provider. Sie hat eine technische Infrastruktur, mit der sie Leute von A nach B befördert, also genauso wie die Access-Provider Informationspakete von A nach B transportieren. Und damit leistet sie den Drogenkonsumenten zumindest Beihilfe. Straflöse Beihilfe zu einer Übertretung, muss man hinzufügen, weil der Betäubungsmittelkonsum durch die Revision des Betäubungsmittelgesetzes 1975 zur Übertretung heruntergestuft wurde (Art. 104 StGB i.V.m. Art. 19a BetmG).

**N:** Mindestens Beihilfe, muss man sagen, weil im Betäubungsmittelgesetz fast alles Täterschaft ist. Hinweisen könnte man auch auf die bekannte Tatsache, dass ein nicht unbeträchtlicher Teil des Drogenhandels um Zürich in den Toiletten der S-Bahn-Wagen erfolgt. Aber

---

6 Die SBB tolerieren Kiffer, *20 minuten*, 15. Januar 2001, 6.

selbst beim Beispiel mit den Kiffern bleiben Zweifel: Die SBB transportieren ja auch Drogen, die noch nicht konsumiert sind, und ob diese Drogen im Sinn von Art. 19a BetmG zum Konsum durch denjenigen bestimmt sind, der sie auf sich trägt (oder zum gemeinsamen Konsum mit anderen), wäre abzuklären. Wenn auch nur einer der Konsumenten Drogen auf sich trägt, die er verkaufen, verschenken oder sonstwie abgeben will, dann transportiert er diese Substanzen. Und dies stellt jedenfalls keine Übertretung, sondern ein Vergehen nach Art. 19 Ziff. 1 BetmG dar. Und damit würde sich die Frage des Transportierens von Drogen auch durch die SBB selbst stellen, ein Delikt, das man nicht nur vorsätzlich, sondern auch fahrlässig begehen kann. Die Kondukteure nehmen ja den Geruch sogar wahr und sagen sich trotzdem, dass es sie nichts angehe.

**S:** Nein, sie sagen das folgende und zwar durch den SBB-Presse-sprecher JEAN-LOUIS SCHERZ: «Machen können wir jedoch nichts.» Und obendrein wird darauf hingewiesen, dass das eine gesellschaftliche Entwicklung sei, die sich weder steuern, noch beeinflussen lasse. Das ist ein ganz ähnliches Problem wie bei den Access-Providern, doch eine Diskussion findet darüber in der Schweiz nicht statt.

**N:** Genau, das ist es. Man könnte auch ein anderes Beispiel nehmen, z.B. die Strassen. Unser Staat baut Strassen im klaren Bewusstsein, dass auf diesen Strassen die Regeln nicht bzw. nur ungefähr beachtet werden. Und auf diesen Strassen (mithilfe dieser Strassen) sterben jedes Jahr ungefähr 600 Personen. Mit dem Argumentationsschema, das gegenüber Providern verwendet wird, würde man sagen: Diese Toten werden in Kauf genommen. Wann sind Sie schon das letzte Mal in eine Verkehrskontrolle geraten? Kann man hier wirklich von Kontrollen sprechen? Und in diesem Argumentationsschema wäre es auch völlig konsistent zu behaupten, dass diejenigen, die die Transportmöglichkeit überhaupt eröffnen, Gefahren schaffen und entsprechend dafür Sorge zu tragen haben, dass diese Gefahren sich nicht realisieren. So betrachtet würde es wohl nicht genügen, Schilder aufzustellen des Inhalts: «Hier gilt 100.» Würde man, was man

dem Provider abverlangt, auch hier verlangen, so würde das bedeuten, dass die Strassenbetreiber hingehen und die geltenden Regeln auch durchsetzen. Von einer Durchsetzung aber sind wir ja ziemlich weit entfernt. Es käme (vorläufig) wohl auch niemand auf die Idee, den Staat strafrechtlich verantwortlich zu machen.

**S:** Also die Rechtslage ist im Moment deshalb verworren, weil ganz verschiedene Standpunkte vertreten werden. Laut einem Gutachten des Bundesamtes für Justiz macht sich ein Access-Provider nach bestehendem Recht strafbar, und zwar entweder als Verbreitungshelfer bei Straftatbeständen, die nicht als Mediendelikte gelten, oder nach Massgabe von Art. 27 StGB bei Mediendelikten. Mit letzterem wollte der Gesetzgeber eigentlich eine Privilegierung der Medienschaffenden erreichen, weil diese Bestimmung die Strafbarkeit auf den Autor der Veröffentlichung beschränkt, falls er gefasst bzw. in der Schweiz vor Gericht gestellt werden kann. Nur wenn der Autor nicht eruiert werden kann, ist eine sekundäre Verantwortung des für die Veröffentlichung Verantwortlichen statuiert, die sich nach Art. 322<sup>bis</sup> StGB richtet. Gemäss Art. 322<sup>bis</sup> StGB ist strafbar, wer es vorsätzlich oder fahrlässig unterlässt, eine strafbare Veröffentlichung zu verhindern. Dieser Ausnahmefall wird nun aber im Bereiche der Internetkriminalität zum Regelfall. Weil der Autor, der ursprüngliche Verantwortliche, in den seltensten Fällen im Inland gefasst werden kann, fällt die strafrechtliche Verantwortlichkeit auf die untergeordneten Glieder im Veröffentlichungsprozess zurück. Als letztes Glied in dieser Kette soll nach dem erwähnten Gutachten des Bundesamts für Justiz auch der reine Zugangsvermittler gelten, der sich folglich strafbar mache, wenn er die Veröffentlichung nicht verhindere. Doch auch dort, wo das Medienstrafrecht nicht anwendbar ist, soll für diese automatisierten Zugangsvermittlungsdienste eine Strafbarkeit wegen Gehilfenschaft möglich sein. Diese Position wird in der Lehre generell angezweifelt. So kommt ein Gutachten der Strafrechtler MARCEL NIGGLI, FRANZ RIKLIN und GÜNTER STRATENWERTH zum konträren Schluss, dass in Bezug auf die Access-Provider schon nach geltendem Recht keine strafrechtliche Verantwortung möglich sei.

**N:** Man muss dazu vielleicht sagen, dass es um einen grundsätzlichen, dogmatischen Ansatz geht. Wieso setzt man an bei jemandem, der die Kommunikation nur ermöglicht. Ein Access-Provider, also ein Zugangs-Provider, hat mit dem Inhalt überhaupt nichts zu tun, er hat ein Vertragsverhältnis mit dem Nutzer. Mit dem schliesst er einen Vertrag. Mit allen andern Beteiligten hat er an sich nichts zu tun. Und wie sehr das Votum der Bundesrätin METZLER eine allgemeine Stimmung wiedergibt, können Sie auch an der Spielbankengeschichte erkennen: Vorweg muss ich erklären, dass es nach dem schweizerischen Spielbankengesetz zulässig ist, zu spielen, aber verboten, eine Spielbank ohne Bewilligung in der Schweiz zu betreiben. Das Betreiben einer Spielbank ohne Bewilligung (und die wird natürlich nicht ohne weiteres erteilt) ist strafbar. Nun hat die schweizerische Spielbankenkommission an alle Access-Provider der Schweiz eine Liste der Spielbanken versandt, die über Internet aus der Schweiz erreichbar sind, und zwar völlig unabhängig von der Frage, welchem Recht diese Spielbanken unterstehen und ob nach dem zuständigen nationalen Recht, dem diese Spielbanken unterstehen, das Betreiben einer Spielbank überhaupt erlaubt sei oder nicht. Die Provider wurden aufgefordert, den Zugang zu diesen Spielbanken zu sperren, unter Verweis auf mögliche strafrechtliche Sanktionen wohlgemerkt. Nach Meinung der Spielbankenkommission werden diese Spielbanken offenbar in der Schweiz betrieben, weil sie übers Internet von hier aus zugänglich sind.

Wenn Sie das dogmatisch durchdenken, dann erkennen Sie, wie heikel diese Position ist. Mir ist nicht bekannt, dass gegen irgend eine dieser Spielbanken ein Strafverfahren eröffnet wurde. Wenn es aber zutrifft, dass die Spielbanken ihr Gewerbe in der Schweiz betreiben, dann müssen doch Strafverfahren eröffnet werden. Im gegenteiligen Fall sind Sie bei ungetreuer Amtsführung, möglicherweise bei der Begünstigung, aber jedenfalls selbst im strafbaren Bereich. Was aber macht die Spielbankenkommission? Sie stellt sich einfach auf den Standpunkt, die Spielbanken würden hier betrieben und die Provider müssten zum Rechten schauen. Die Betreiber der Spielbanken



hingegen werden gar nicht ins Recht zu fassen versucht. Warum nicht? Nun, weil dann eben die eigentliche Schwierigkeit offenbar würde. Ein Spielbanken-Betreiber in den Staaten oder in Spanien oder einem beliebigen anderen Land, der sich nach dem jeweilig anwendbaren nationalen Recht korrekt verhält, wird sagen «Ich unterstehe dieser Rechtsordnung und verhalte mich korrekt. Das Problem besteht nicht in meiner Tätigkeit, das Problem bilden vielmehr die spielenden Schweizer.» Das hatten wir auch kurz vorher andiskutiert. Wenn sich jemand physisch an den Ort einer Spielbank begibt und dort spielt, dann ist das Ganze ja völlig legal. Es kommt nur darauf an, wo und wie gespielt wird.

**S:** Ich möchte auch noch auf einen anderen Punkt hinweisen. Mit der momentanen Rechtsunsicherheit entsteht die Gefahr, dass eine Fehlentwicklung einsetzen könnte. Sie verleitet nämlich private Organisationen, sich diese, sagen wir, relativ schwammige Rechtslage zu Nutze zu machen, indem sie von Access-Providern unter Androhung von öffentlichen Medienaktionen und einer Strafanzeige die Sperrung von illegitim erscheinenden Websites fordern, also sozusagen eine private Sperrverfügung oder Abmahnung zustellen. Sie haben sicher vom Front14.org-Fall gehört, bei dem die «Aktion Kinder des Holocaust» drei grössere Provider in der Schweiz angeschrieben und aufgefordert hat, den Zugang zu Front14.org zu sperren, ansonsten eine Anzeige erfolge. Dem haben dann alle drei Access-Provider aus ethischen Gründen Folge geleistet. Es ist aus rechtsstaatlicher Sicht aber höchst problematisch, wenn Access-Provider auf Druck welcher privaten Interessenvertretungen auch immer, mehr oder weniger willkürlich ihren Kunden, die Bürger eines demokratischen Staates sind, den Zugang zu bestimmten Seiten verwehren sollten.

Sie sehen, es geht um die Problematik der Privatzensur. Auch wenn solche Abmahnungen vielleicht in Bezug auf diese rassistischen Websites verständlich erscheinen, mag man nicht recht glücklich werden mit der Vorstellung, dass in Zukunft beliebige Private die

Access-Provider zu Zensurmassnahmen veranlassen könnten. Weil sich aber niemand gerne einer Strafverfolgung mit unkalkulierbarem Ausgang aussetzt, die noch dazu für das Image einer Unternehmung äussert negative Konsequenzen hat, resultiert ein sogenannter «chilling effect», d.h. im Zweifel wird alles einmal gesperrt. Deshalb ist es sehr wichtig, die Reichweite der Strafbarkeit bei Internetkommunikation schnell gesetzlich zu regeln, wie das mit einer Motion von Ständerat THOMAS PFISTERER, die der Ständerat am 6. März 2001 debattiert und angenommen hat, vorgeschlagen wird. Auch der Bundesrat stimmt grundsätzlich mit dem Anliegen dieser Motion überein. Der Motion liegt ein Revisionsvorschlag für das Strafbuch von Marcel Niggli und mir zugrunde, den man inhaltlich etwas erläutern sollte.<sup>7</sup>

**N:** Gut, also unser Vorschlag ist relativ simpel. Es geht darum, dass man die strafrechtliche Verantwortlichkeit der drei grundsätzlich unterschiedlichen Typen von Providern ausdrücklich regelt. Dass man festlegt, welche Verantwortlichkeiten bestehen, wenn nur der Zugang vermittelt wird, wenn gehostet wird (wenn also jemand aufgrund eines Vertragsverhältnisses einem anderen seine Computer zur Verfügung stellt zwecks Bereithaltung von bestimmten Informationen), oder wenn Informationen eingespeist werden. Bei dieser dritten Kategorie handelt es sich typischerweise um die Autoren, die ohnehin der klassischen strafrechtlichen Haftung unterliegen. Was wir für sinnvoll erachten würden, wäre eine Anknüpfung am Medienstrafrecht und zwar deshalb, weil sich eben Internet und Medienstrafrecht überschneiden. Ein Beispiel: Die NZZ und ihre Mitarbeiter unterstehen der medienstrafrechtlichen Regelung. Wenn für Internet-Publikationen eine völlig andere Regelung bestünde, dann würde das bedeuten, dass die Mitarbeiter der NZZ nur so lange dem Medienstrafrecht unterstünden, als die NZZ nicht aufs Netz ginge. Mit der Publikation über Internet würde die medienstrafrechtliche Regelung ihre Geltung verlieren. Das kann nicht richtig sein. Da

---

7 [www.parlament.ch/afs/data/d/gesch/2000/d\\_gesch\\_20003714.htm](http://www.parlament.ch/afs/data/d/gesch/2000/d_gesch_20003714.htm) (Stand: 16.5.2001).



würden alle Journalisten natürlich Sturm laufen und zurecht betonen, dass das Medienstrafrecht kürzlich revidiert wurde und nicht einfach derart ausgehebelt werden kann, dass jeder, der in irgend einer Art und Weise in diesen Medienunternehmen mitarbeitet, wieder den üblichen Regeln der Teilnahme untersteht, einfach nur deshalb, weil die NZZ auf das Internet portiert wird.

**S:** Als Einwand gegen eine solche Regelung, die sich an die Richtlinie der Europäischen Gemeinschaft über den elektronischen Geschäftsverkehr<sup>8</sup> anlehnt, wird immer wieder aufgeworfen, dass ein Regelung, welche die reine Zugangsvermittlung für straflos erkläre, dazu führe, dass man überhaupt nichts mehr gegen die Internetkriminalität unternehmen könne.

Die Access-Provider als letzter inländischer Anknüpfungspunkt für eine Strafverfolgung, so die Bundesrätin METZLER in ihrer Stellungnahme auf die Motion Pfisterer, ginge uns verloren. Darauf ist zu antworten: Nein, der Anknüpfungspunkt geht zwar im strafrechtlichen Kontext verloren, aber es ist bezüglich der Verpflichtungen zur Entfernung oder Sperrung der Nutzung von Informationen ein Vorbehalt zugunsten der allgemeinen Erlasse des Bundes und der Kantone vorgesehen. Wie übrigens auch in allen europäischen Umsetzungsgesetzen zur E-Commerce-Richtlinie bleiben verwaltungsrechtliche und im Privatrecht vorgesehene Sperrverfügungen oder andere Massnahmen weiterhin möglich.

Das heisst, es handelt sich nicht mehr um ein strafrechtliches Sanktionieren eines bestimmten tatbestandsmässigen, rechtswidrigen und schuldhaften Verhaltens, sondern um Prävention, und das ist Polizeirecht im weiteren Sinne. Es geht dabei eigentlich um verwaltungsrechtliche Gefahrenabwehr. Sperrverfügungen gegen Access-Provider wären also weiterhin zulässig, wenn ein Gefahrenherd im Inter-

---

8 Vgl. Art. 12ff. der Richtlinie 2000/31/EG des Europäischen Parlaments und des Rates vom 8. Juni 2000 über bestimmte rechtliche Aspekte der Dienste der Informationsgesellschaft, insbesondere des elektronischen Geschäftsverkehrs, im Binnenmarkt, ABl. L 178 vom 17.7.2000, S. 1ff.

net festgestellt wird und die Voraussetzungen für einen staatlichen Eingriff vorliegen, also eine gesetzliche Grundlage, ein öffentliches Interesse und die Verhältnismässigkeit<sup>9</sup> der gefahrabwehrenden Massnahme. Unter diesen Voraussetzungen sind die Access-Provider weiterhin zur Kooperation verpflichtet. Falls die Sperrverfügung von der zuständigen Behörde mit einer Strafdrohung nach Art. 292 StGB<sup>10</sup> verbunden wird, könnte eine Widerhandlung des Access-Providers sogar wieder zu einer strafrechtlichen Sanktionierung führen. Ein renitenter Access-Provider könnte also durchaus noch ins Recht gefasst werden. Das wäre dann eine saubere Lösung, wie sie auch die Provider selber anstreben.

**N:** Die Frage ist natürlich, wieso sollte das im Strafgesetzbuch geregelt werden? Deutschland z.B. hat das in einem separaten Gesetz getan und zwar mittels einer sog. Horizontalregelung. Darin wird einfach festgelegt, was für alle Tele-Dienste gilt, und zwar im Hinblick auf sämtliche Rechtsbereiche. Ein solcher Ansatz erscheint uns hochproblematisch und zwar deshalb, weil bis zu einem gewissen Grade Strafbarkeitseinschränkungen notwendig sind, also spezielle Bedingungen der Strafbarkeit der verschiedenen Kategorien von Providern. Die Strafbarkeit nach den allgemeinen Zurechnungsregeln des Strafgesetzbuches kann aber kaum über einen Nebenerlass eingeschränkt werden. Sie kann ohne weiteres ergänzt und erweitert werden, was wir ja in mehr als 200 Erlassen in der Schweiz auch getan haben. Aber eine einschränkende oder grundsätzlich andere Regelung erscheint heikel, weil das ja bedeuten würde, dass der einschränkende Erlass bzgl. der Strafbegründung höher steht als das Strafgesetzbuch.

Die Idee, dass wir einfach alles mit Internet-Bezug in einem einzigen Erlass regeln – wie z.B. in Deutschland – halten wir noch aus anderen Gründen für verfehlt. Auch jetzt schon nämlich (also ohne Bezug zum Internet) unterscheiden wir typischerweise nach Rechtsbe-

---

9 Vgl. Art. 36 BV.

10 Ungehorsam gegen amtliche Verfügungen, Art. 292 StGB.

reichen: Es kann ein Täter zivilrechtlich verantwortlich sein, aber nicht strafbar. Er kann strafbar sein, aber verwaltungsrechtlich oder zivilrechtlich nicht belangbar. Natürlich kann das im einzelnen Fall zu Schwierigkeiten führen, aber grundsätzlich gilt eben nicht in allen Rechtsbereichen dasselbe. Zu glauben, nur weil es sich um Internet handelt, also um etwas technisch Komplexes, man könne alle rechtlichen Bedingungen in eine einheitliche Gesetzesvorlage packen, ist nach unserem Dafürhalten falsch. Falsch insbesondere auch deshalb, weil die Dogmatik der einzelnen Bereiche, die Begrifflichkeit, eine jeweils andere ist. Deshalb geht auch unser Vorschlag dahin, dass eine mögliche Einschränkung der Strafbarkeit analog zu derjenigen im Medienstrafrecht, nicht bedeuten kann, dass verwaltungsrechtlich oder zivilrechtlich keine entsprechenden Massnahmen möglich seien. Eine Beschränkung der Strafbarkeit gründet also nicht etwa darauf, dass man da nichts machen könnte (Stichwort SBB und Kiffer), sondern stellt den Versuch einer Regelung dar. Allerdings einer bescheidenen Regelung, die sich nicht anmasst, sämtliche Fragen in einem Aufwasch zu beantworten.

**S:** In der Schweiz besteht zudem zeitliche Dringlichkeit. Die Europäische Union hat das Problem der Verantwortlichkeit für Tele Dienste sehr früh erkannt und bereits im Juni 2000 die schon mehrfach erwähnte E-Commerce-Richtlinie verabschiedet. Diese muss von den Mitgliedsstaaten bis spätestens 17. Januar 2002 in die nationale Rechtsordnung umgesetzt werden. Besonders die grossen Staaten, wie Frankreich, England, Deutschland, die sich als Standorte für den E-Commerce profilieren wollen, sind jetzt gerade an der Verabschiedung der notwendigen gesetzlichen Anpassungen. In Deutschland hat die Bundesregierung bereits das entsprechende Umsetzungsgesetz in den Bundestag geschickt. Frankreich und Grossbritannien wollen die Umsetzung bis Oktober 2001 verwirklichen. Wenn jetzt die Schweiz nachhinken würde, käme es zu einer Situation, in der sich mancher Internet-Service-Provider fragen dürfte, ob er sich nicht besser in einem Land niederlassen solle, in dem die rechtlichen Rahmenbedingungen kalkulierbarer sind. Für die Inter-

net-Service-Provider ist ein Abzug nach Konstanz oder ins nahe Ausland technisch völlig problemlos. Es ist auch so, dass der von der E-Commerce-Richtlinie abgesteckte Rahmen für ganz Europa eine einheitliche Regelung bringt, die von den Mitgliedsstaaten weder verschärft noch abgeschwächt werden kann. Ein einheitlicher europäischer Standard wird folglich bald Realität werden.

**N:** Man kann das Ganze ja gedanklich durchspielen. Die Bundespolizei z.B. befürwortet wohl die Strafbarkeit der reinen Zugangsvermittler. Das würde natürlich die Strafverfolgung erleichtern, weil die Provider hier ansässig sind. Gegenwärtig etwa findet das z.B. so statt, dass man eben einen Brief schreibt und auf bestimmte fragliche Informationen hinweist und die Provider einlädt, darüber nachzudenken, ob diese Informationen nicht gesperrt werden müssten. Ein solches Vorgehen bewirkt bei den Providern typischerweise Verunsicherung. Muss nun gesperrt werden oder nicht? Eine Frage, auf die es natürlich mangels der Eröffnung eines Strafverfahrens gegen die Autoren (Content-Provider) keine eindeutige Antwort geben kann. Das erscheint als zweifelhafter Weg. Nehmen wir an, dass sich die Provider infolge dieser Zweifel aus der Schweiz ins europäische Umland zurückziehen. Was übrig bliebe, wäre die Swisscom, die ja nicht weg kann. Die Swisscom ihrerseits würde dann wohl ihre Leitungen an die im Ausland ansässigen Provider vermieten. Und in einer solchen Konstellation nun wird die Problematik überdeutlich: Zuerst gehen wir von der Strafbarkeit des Autors über zu derjenigen des Providers, der nur den Zugang vermittelt. Hat aber der Provider seinen Sitz und seine Computer im Ausland, dann ist eine zusätzliche Erweiterung notwendig, nämlich die Erweiterung der Strafbarkeit hin zu demjenigen, der die Leitung, also das physische Netz, vermietet. In dieser Konstellation wird deutlich sichtbar, dass wir den Strafbarkeitsbereich schon sehr sehr stark erweitern müssen, um tatsächlich jemanden in der Schweiz strafbar werden zu lassen. Wenn wir das in anderen Bereichen auch täten, dann wären die meisten von uns mit Strafe bedroht.

**S:** Was das Vollzugsdefizit anbelangt, ist auch noch zu erwähnen, dass eine zentrale Behörde für die Strafverfolgung notwendig ist. Die Cyber-Crime Convention sieht im Entwurf 7x24-Stunden-Schnittstellen auf nationaler Ebene vor, d.h. Ansprechstellen, die 7 Tage pro Woche und 24 Stunden besetzt sein müssen, damit ein schneller internationaler Informationsaustausch gewährleistet werden kann. Gerade in der Schweiz, wo die Strafverfolgung im wesentlichen föderalistisch geregelt ist, wäre es dringend geboten, bei der Bundespolizei eine zentrale Abteilung für Internetkriminalität mit entsprechenden Fachleuten einzurichten. Dass das nicht billig ist, kann man an den Bemühungen der anderen Länder wie Grossbritannien, Japan, den USA und Deutschland ablesen. Grossbritannien hat seit dem letzten Jahr eine zentrale National Hi-Tech Crime Unit (NHT-CU) aufgebaut, die ab April 2001 von einem geheimen Ort in London aus im Einsatz steht. Zur Schaffung der notwendigen Infrastruktur hat das Home Office ein Budget von £ 25 Mio. vorgesehen.<sup>11</sup> Es besteht ein riesiger Nachholbedarf an Fachkräften und modernen Computereinrichtungen. Auch die Schweiz bedarf zunächst einmal einer effizienten Infrastruktur, wobei das entsprechende Know-how durchaus auch in Zusammenarbeit mit den Internet-Providern aufgebaut werden kann. Ähnliche Entwicklungen sind in den USA, Japan und Deutschland festzustellen. Deshalb sieht der Motionstext vor, eine Bundeskompetenz für den Bereich der Netzwerkkriminalität einzuführen.

**N:** Man müsste vielleicht noch eine Anmerkung machen: Es kommt immer wieder der Vorschlag, solche Schnittstellen seien nicht nötig, das Problem liesse sich vielmehr über Hotlines der Provider selbst lösen. Solche Hotlines würden den Providern ermöglichen, sich selbst zu organisieren und die Nutzer würden die Basis-Informationen mittels Anruf bereitstellen. Diese Hotlines wären also quasi Call-Center der Provider. Basierend auf den Informationen der Hotlines könnten dann die Provider die entsprechenden Informationen

---

11 Vgl. den Bericht in *BBC News*: New force to tackle cybercrime, 18 April 2001, abrufbar unter: [http://news.bbc.co.uk/1/hi/english/uk/newsid\\_1282000/1282816.stm](http://news.bbc.co.uk/1/hi/english/uk/newsid_1282000/1282816.stm) (Stand: 20.5.01).



vom Netz nehmen oder eben nicht. Nur, meine Damen und Herren, das ist nicht nur etwas naiv, sondern auch rechtsstaatlich bedenklich. Klar, jeder und jede von uns erkennt ein kinderpornographisches Bild, wenn er oder sie ein solches Bild vor sich hat. Nur, es gibt ganz viele Bereiche der Pornographie, wo das nicht mehr ganz so einfach ist. Oder denken Sie an die Rassendiskriminierung oder die Gewaltdarstellungen. Hier weiss ein Laie kaum je, ob eine entsprechende Darstellung oder Information zulässig sei oder nicht. Mittels Hotlines würde faktisch die staatliche Verantwortung einer Entscheidung darüber, was strafrechtlich zu verfolgen sei oder nicht, weitergegeben an die Privaten: Die Privaten müssten selbst zum Rechten schauen. Und wenn sie Pech hätten oder nicht genau hinschauten, dann würden sie eben strafbar. Das kann keine korrekte Argumentation sein. Auch im Bereich des Internet sollte doch die gegenwärtig gültige Strafrechtsdogmatik Anwendung finden. Wir geben uns doch Mühe, Gesetze zu machen, die es erlauben, aufgrund des Gesetzestextes halbwegs zu bestimmen, was erlaubt sei und was nicht. Dies gelingt uns vielleicht nicht immer und vielleicht auch immer weniger. Nur: Die Anwendung der geltenden Gesetze bleibt eben staatliche Kernkompetenz. Wenn der Staat die Strafverfolgungskompetenz von vorneherein an Private delegiert, weil er sich für inkompetent deklariert, dann sind wir doch auf einem seltsamen Weg. Natürlich würde eine effektive Strafverfolgung bzgl. Internet-Straftaten auch Kosten verursachen, aber diese Kosten sollten wir zu decken bereit sein, wenn uns an dieser Verfolgung liegt. Sie einfach an Private weiterzugeben, halten wir schon für zweifelhaft.

**S:** Ich glaube, wenn wir langsam gegen das Ende zukommen, ist noch einmal das Augenmerk auf das hauptsächliche Problem zurückzulenken. Wir haben hier eine lange Diskussion über einen Nebenschauplatz geführt, nämlich denjenigen der Strafbarkeit von Host- und Access-Providern, die im Grunde nur automatisierte Prozesse der Datenverbreitung und Datenbereithaltung anbieten. Aber eigentlich müsste man, wie üblicherweise im Strafrecht, beim Urheber der strafbaren Informationen ansetzen. Man muss also versu-

chen, dort den Content, die eigentliche Information zu verfolgen, wo er herkommt, und die Autoren ins Recht zu nehmen. Das ist nicht ganz so einfach, aber unmöglich ist es nicht. Erste Ansätze sind in der Umsetzungsphase. Wie gesagt, die Internationalität kann durch einheitliches materielles Strafrecht entschärft werden. Es gibt in der Cyber-Crime Convention auch einige sinnvolle prozessrechtliche Regelungen. Einige darunter sind zwar sehr umstritten, weil z.B. keine Einigkeit darüber besteht, wie weitgehend die Überwachung des Internetverkehrs möglich sein soll, doch sind wichtige Harmonisierungsbestrebungen im Bereich der Beweismittelsicherung und der internationalen Rechts- und Amtshilfe in den Entwurf eingeflossen. Das ist ein erster Ansatzpunkt. Wichtig ist hierbei, dass der Fokus wieder dorthin gewendet wird, wo die Straftäter sind. Und diesen ist nur mit internationaler Kooperation beizukommen, auch wenn das aus der Perspektive eines nationalstaatlichen Strafrechts ein bisschen ungewohnt erscheint.

**N:** Noch einmal am Beispiel: Wenn wir die Argumentation, die im Hinblick auf das Internet immer wieder aufkommt, in den analogen, normalen Lebensbereich transponieren, dann kann man nur staunen: Wenn jemand aus dem Ausland einer Person in der Schweiz einen strafbaren Inhalt zusendet, käme wohl niemand auf die Idee, den Postbeamten für die Sendung bzw. den Inhalt verantwortlich werden zu lassen. Und dies auch dann nicht, wenn der Autor der Sendung im Ausland sitzt und seine Verfolgung deshalb als schwierig erscheint. Im Bereich der Brief- oder Paketpost gilt ja das genaue Gegenteil: Hier schützen wir das Briefgeheimnis. Der Postbeamte würde selbst strafbar, wenn er ein bisschen nachschaute, was so in den Briefen enthalten ist. Also nur schon das Lesen einer Postkarte ist etwas Heikles, das uns in unseren Empfindungen betrifft, aber wenn der Postbote auch noch unsere Briefe aufmachen würde, dann wäre er zweifelsfrei im strafbaren Bereich.

Und das ist, worum es geht, meine Damen und Herren. Dass wir eben, wenn wir eine neue technische Struktur haben, versuchen



müssen, diese technische Struktur gemäss ihren Eigenheiten zu regeln. Dazu bestehen auch Möglichkeiten. Zum einen erscheint deutlich, dass wir uns – wie Christian Schwarzenegger das bereits gesagt hat – nicht primär auf die Übermittler, sondern auf die Täter fokussieren sollten. Wir müssen versuchen z.B. die Rechtshilfe zu verbessern. Das kann man über Abkommen tun. Selbst mit den Amerikanern können wir Abkommen schliessen, vielleicht nicht über die Inhalte, die in den Staaten für legal erachtet werden, aber z.B. im Hinblick auf die Herausgabe von Logs: Wenn wir wissen, wann sich wer von wo aus auf den Server eingeloggt hat, um das fragliche Material einzuspeisen, dann wären wir schon einen grossen Schritt weiter, weil damit die Zuständigkeit unserer Rechtsordnung feststünde, wenn der Täter von hier aus gehandelt hat. Und wenn hin und wieder Kritik an den Strafverfolgungsorganen laut wird, weil die zu wenig täten, dann muss man darauf verweisen, dass die Polizei eben dazu da ist, Straftäter zu verfolgen, nicht Postbeamte.

## Literaturauswahl

- BUNDESAMT FÜR JUSTIZ: Frage der strafrechtlichen Verantwortlichkeit von Internet-Access-Providern gemäss Art. 27 und 322<sup>bis</sup> StGB, Gutachten des Bundesamtes für Justiz vom 24. Dezember 1999, VPB 2000, 820ff.
- BURI, UELI: Übersicht über die Rechtsprechung im Bereich Informatik und Recht: *Internet-Recht, Jusletter*, 20. November 2000 [www.weblaw.ch].
- HEINZELMANN, PETER L./OCHSENBEIN, ANDREAS: Strafrechtliche Aspekte des Internet, *Kriminalistik* 1998, 513ff., 599ff.
- NIGGLI, MARCEL ALEXANDER: Nationales Strafrecht vs. Globales Internet – in: AUF DER MAUER, ROLF/HILTY, RETO M./WEBER, ROLF H. (Hrsg.): Geschäftsplattform Internet II – Internet und Inhalte, Zürich 2001 [im Druck].
- NIGGLI, MARCEL ALEXANDER/RIKLIN, FRANZ/STRATENWERTH, GÜNTER: Die strafrechtliche Verantwortlichkeit von Internet-Providern. Ein Gutachten, Sonderausgabe MediaLex 2000.
- RIKLIN, FRANZ: Information Highway und Strafrecht – in: HILTY, RETO M. (Hrsg.): Information Highway, Beiträge zu rechtlichen und tatsächlichen Fragen, Bern und München 1996, 559ff.
- SCHLEIMINGER, DORRIT/METTLER, CHRISTOPH: Strafbarkeit der Medienverantwortlichen im Falle der Rassendiskriminierung. Art. 27, Art. 261<sup>bis</sup> Abs. 4 StGB, Bemerkungen zu BGE 125 IV 206ff., AJP 2000, 1039ff.
- SCHWARZENEGGER, CHRISTIAN: Der räumliche Geltungsbereich des Strafrechts im Internet. Die Verfolgung von grenzüberschreitender Internetkriminalität in der Schweiz im Vergleich mit Deutschland und Österreich, ZStrR 2000, 109ff.
- SCHWARZENEGGER, CHRISTIAN: Gefangen im Spinnennetz der Strafjustiz? Die strafrechtliche Bewertung von Links, *Neue Zürcher Zeitung*, 30. Juni 2000, Nr. 150, 71.
- SCHWARZENEGGER, CHRISTIAN: Abstrakte Gefahr als Erfolg im Strafanwendungsrecht – Ein leading case zu grenzüberschreitenden Internetdelikten, sic! 2001, 3/2001, 240ff.

- SIEBER, ULRICH: Verantwortlichkeit im Internet, Technische Kontrollmöglichkeiten und multimediarrechtliche Regelungen, Zugleich eine Kommentierung von § 5 TDG und § 5 MDStV, München 1999.
- WEBER, ROLF H.: E-Commerce und Recht. Rechtliche Rahmenbedingungen elektronischer Geschäftsformen, Zürich 2001.
- WEBER, ROLF H./UNTERNÄHRER, ROLAND: Wirtschaftsterrorismus im Internet – in: ACKERMANN, JÜRG-BEAT/DONATSCH, ANDREAS/REHBERG, JÖRG (Hrsg.): Festschrift Niklaus Schmid, Zürich 2001, 365ff.
- WEISSENBERGER, PHILIPPE: Zum Begehungsort bei Internet-Delikten, ZBJV 1999, 703ff.
- WIDMER, URSULA/BÄHLER, KONRAD: Rechtsfragen beim Electronic Commerce. Sichere Geschäftstransaktionen im Internet. Zürich 1997 (2. unveränderte Aufl., Zürich 2000).

