ÖJZ

Österreichische Juristen-Zeitung

HEFT 4 | 18. FEBRUAR 2002 | 57. JAHRGANG

ISSN 0029-9251

MANZ

Univ.-Ass. Dr. Stefan Ebensperger, Innsbruck

Die Verbreitung von NS-Gedankengut im Internet und ihre strafrechtlichen Auswirkungen

unter besonderer Berücksichtigung des E-Commerce-Gesetzes

Zum Inhalt: *Das Internet wird bekanntlich vielfach auch zu kriminellen Aktivitäten genutzt, ua in zunehmendem Ausmaß auch zur Verbreitung neonazistischer, rechtsextremer, rassistischer, antisemitischer, ausländerfeindlicher und Gewalt verherrlichender Inhalte. Der folgende Beitrag befasst sich mit den strafrechtlichen Aspekten der Verbreitung, dem Zugänglichmachen und der Äußerung derartiger Internet-Inhalte, wobei besonders auf neonazistische Aktivitäten eingegangen wird.*

Inhaltsübersicht

I. Einleitung

A. Problemdarstellung

Das Internet als ständig wachsendes Kommunikations-, Kommerz- und Informationsmedium ist in zunehmendem Ausmaß auch Schauplatz von kriminellen Aktivitäten. Prinzipiell können im Internet alle strafbaren Handlungen begangen werden, die keinen direkten Körperkontakt zwischen Opfer und Täter verlangen[1]). So kommt es zB zu Datenbeschädigungen[2]), Betrug, Hehlerei, Ehrenbeleidigungen oder der Verbreitung von kriminellen Inhalten[3]). An **kriminellen Inhalten**[4]) werden überwiegend Kinderpornographie[5]), immer häufiger aber auch neonazistische[6]), rechtsextreme, rassistische, antisemitische, revisionistische, Gewalt verherrlichende und ausländerfeindliche Inhalte verbreitet[7]). Die folgende Untersuchung befasst sich mit den strafrechtlichen Aspekten der Verbreitung, dem Zugänglichmachen und der Äußerung solcher Inhalte im Internet (**„Verbreitungs- und Äußerungsdelikte"** oder auch „Kommunikationsdelikte"). Besonders eingegangen wird dabei auf neonazistische Aktivitäten.

Das Internet spielt eine immer größere Rolle als Propaganda- und Rekrutierungsmedium der rechtsextremen Szene: Die Ausbreitung **neonazistischer Homepages** wird immer Besorgnis erregender[8]). Rechtsextremisten gestalten ihre Seiten zunehmend professioneller und aggressiver. Sie rufen zum Rassenhass auf und propagieren die Gewalt insb gegen ausländische Mitbürger. Auf einigen Seiten finden sich „schwarze Listen", in denen politische Gegner („Feinde des Reichs") benannt und deren Adressen veröffentlicht werden, zT mit der Aufforderung zum Mord an diesen Personen[9]). Daneben existieren Seiten mit Lügen über den Holocaust **(„Auschwitz-Lüge")** unter Anführung „wissenschaftlicher" Beweise. Einige Netzanbieter stellen auch Texte mit (neo-)nazistischen Inhalten zum Downloaden zur Verfügung, wie zB Hitlers „Mein Kampf"[10]) durch das „Thule-Net". Die Anzahl rechtsextremer deutschsprachiger Internet-Seiten hat sich von 1999 bis 2001 auf **etwa 1000** mehr als verdreifacht[11]). Dazu kommen noch einschlägige Seiten in anderen Sprachen. Der Rechtsradikalismus hat durch das Internet eine völlig neue Dimension erlangt[12]).

Neonazistische Inhalte finden sich aber nicht nur auf Homepages, sondern auch in **Newsgroups**[13]) (zB „alt.skinheads"), **Diskussionsforen,** e-mails[14]) und in virtuellen **Chatrooms.** Dort werden beispielsweise Diskussionsteilnehmer zum Einsatz von Gewalt zur Durchsetzung politischer Ziele aufgefordert[15]). Daneben werden auch Hakenkreuzbilder oder ähnliche Symbole *(„clip-arts")* zum Gestalten eigener Nazi-Homepages[16]) und sogar **Nazi-Computer-Spiele** zum download angeboten. So existiert zB eine Cover-Version der „Moorhuhn-Jagd", bei dem die Spieler statt auf Hühner auf Juden schießen[17]). Auch Musikstücke (im sog „**mp3**-Format") mit hetzerischen Texten werden angeboten, die sich Interessenten (meist kostenlos) auf die Festplatte laden können. Das Angebot reicht vom *Horst-Wessel*-Lied bis hin zu Skinhead-Musik. Die Internet-Börse *Napster* geriet im Dezember 2000 in die Schlagzeilen, als bekannt wurde, dass über diesen Dienst viele Neonazi-Musiktitel getauscht werden, deren Texte zum Mord aufrufen[18]).

---

[1]) Das gilt aber auch nur für den unmittelbaren Täter; bestimmen oder beitragen (§ 12 zweiter und dritter Fall StGB) kann man über das Internet theoretisch zu allen Straftaten.

[2]) Va durch Computerviren (vgl zB den Fall des „I-love-you-Virus" im Mai 2000).

[3]) Eingehend zu den kriminellen Aktivitäten im Internet: *Schmölzer,* Internet und Strafrecht, in StPG 25, 129 (140) mwN.

[4]) Als Inhalte gelten insb Texte und Bilder, aber auch Filme, Musikdateien, Spiele oder Programme. Das ECG verwendet für Inhalte den Begriff der „Information" (vgl zB § 16 Abs 1 ECG).

[5]) Siehe dazu zB *Auer/Loimer,* Zur Strafbarkeit der Verbreitung von Kinderpornographie über das Internet, ÖJZ 1997, 613 und *Freund,* Die Strafbarkeit von Internetdelikten. Eine Analyse am Beispiel pornographischer Inhalte (1998).

[6]) Unter „neonazistisch" wird hier eine NS-Wiederbetätigung iSd VG verstanden. Zur Verbreitung von neonazistischen Inhalten im Internet: Stiftung Dokumentsarchiv des österreichischen Widerstandes (Hrsg), Das Netz des Hasses, Rassistische, rechtsextreme und neonazistische Propaganda im Internet (1997); *Schröder,* Neonazis und Computernetze (1995) uva.

[7]) *Mayer-Schönberger,* Das Recht am Info-Highway (1998) 91 ff.

[8]) Siehe dazu zB (Deutsches) Bundesministerium des Inneren (Hrsg), Verfassungsschutzbericht 2000, 3.1.

[9]) Siehe dazu zB Süddeutsche Zeitung vom 12. 8. 1999, 43.

[10]) Dieses „Werk" kann beim Internet-Buchhändler *Amazon* ganz normal bestellt werden; lediglich nach Deutschland wird es nicht ausgeliefert.

[11]) Der Standard, 22. 8. 2001.

[12]) *Holznagel/Kussel,* Möglichkeiten und Risiken bei der Bekämpfung rechtsradikaler Inhalte im Internet, MMR 2001, 347.

[13]) Newsgroups sind Diskussionsgruppen über die unterschiedlichsten Themen, an denen sich jeder Nutzer des Internets beteiligen kann. Ein Nutzer schreibt eine Frage und schickt (engl: *postet*) sie an die Newsgroup. Andere Nutzer lesen die Mitteilung und antworten darauf. Die Newsgroups befinden sich im sog *„Usenet"*, einem neben dem Internet existierendem Netz.

[14]) E-mails spielen für die vorliegende Untersuchung (Neonazismus) eine weniger bedeutende Rolle, da die einschlägigen Bestimmungen des VG und des StGB an die *öffentliche* Verbreitung bzw an das Zugänglichmachen für eine größere Anzahl von Personen anknüpfen. Dieses Erfordernis wird bei der Versendung einzelner e-mails nicht erreicht werden; anders dagegen, wenn ein neonazistischer Inhalt (als Massensendung) einer entsprechenden Anzahl von Leuten zugesandt wird. Besondere Bedeutung kommt den e-mails dagegen im Bereich der Kinderpornographie zu: § 207a StGB stellt ua das Anbieten, (einem anderen) Verschaffen oder Zugänglichmachen von Kinderpornos unter Strafe, was auch via e-mail begangen werden kann.

[15]) Siehe dazu zB (deutsches) Bundesministerium des Inneren (Hrsg), Verfassungsschutzbericht 1999, 111 ff.

[16]) *Holznagel/Kussel,* MMR 2001, 347.

[17]) *Neitzel,* Filtersoftware gegen Rechts ist das Eine – Erziehung zu Toleranz das Andere, Frankfurter Rundschau 20. 10. 2000.

[18]) Bertelsmann verurteilt Missbrauch von Napster, dpa 19. 12. 2000.

Problematisch an dieser Situation ist, dass – abgesehen von Deutschland – in den meisten Staaten kein dem österr VerbotsG (VG) entsprechendes Gesetz existiert, das die Verbreitung neonazistischer Inhalte unter Strafe stellt. So ist zB in den **USA** (als Heimat vieler rechtsextremer Gruppierungen) die Verbreitung rechtsextremen Gedankenguts durch das nahezu schrankenlose Grundrecht auf Rede- und **Meinungsfreiheit** geschützt. Wer also zB auf einem amerikanischen Server[19]) Seiten mit der Auschwitzlüge ins Internet stellt, ist auf Grund der *Freedom of Speech* (geregelt im *First Amendment* der US-Verfassung) nach amerikanischem Recht **nicht strafbar.** Das *First Amendment* sieht keine Gesetzesvorbehalte vor und bindet sowohl den Bundesgesetzgeber als auch die Gesetzgeber der Einzelstaaten. Eine Pönalisierung der Verbreitung von nationalsozialistischem Gedankengut widerspräche der derzeitigen Interpretation[20]) und würde als Zensur verstanden werden. Eine diesbezügliche Einschränkung der Meinungsfreiheit in den USA ist in nächster Zukunft nicht zu erwarten[21]). Selbst dann, wenn es einmal zum Löschen oder Sperren einer Seite durch den Provider kommt, bedeutet das nicht, dass diese Seite damit automatisch „aus dem Verkehr gezogen" ist: IdR hat der Urheber sie gespeichert und kann sie unter einer neuen Internetadresse auf einen oder mehrere andere Server **„spiegeln",** also kopieren. Zudem ist es heute möglich (und in neonazistischen Kreisen auch üblich) Inhalte **anonym** im Internet zu verbreiten, sodass im Fall einer Strafverfolgung der Urheber oft nicht ausgeforscht werden kann[22]). Problematisch ist schließlich auch die Frage nach dem Täterkreis: Soll/kann nur derjenige bestraft werden, der kriminelle Inhalte im Internet verbreitet hat (Urheber), oder auch derjenige, der auf solche Seiten via Hyperlinks verweist (Linksetzer), der die technischen Voraussetzungen liefert, um die Inhalte im Netz zu verbreiten (Provider) oder (auch) derjenige, der die Inhalte liest (Konsument)[23])?

In der vorliegenden Untersuchung sollen zunächst die strafrechtlichen Konsequenzen für den Urheber neonazistischer und ähnlicher Inhalte geklärt und dabei kurz auf die einschlägigen Bestimmungen im VG, StGB, und im Verwaltungsstrafrecht eingegangen werden. Im nächsten Teil wird eine mögliche strafrechtliche Haftung des Providers, des Linksetzers und des Konsumenten geprüft. Schwerpunkt bilden hier die einschlägigen Bestimmungen des seit 1. 1. 2002 in Kraft befindlichen E-Commerce-Gesetzes (ECG)[24]). Den Abschluss bilden Überlegungen über die Anknüpfungspunkte inländischer Gerichtsbarkeit sowie über die Möglichkeiten der (zukünftigen) rechtlichen und technischen Bekämpfung des Neonazismus im Internet.

B. Täterarten

Rechtswidrige Inhalte im Internet sind nur strafbar, wenn der Täter den Tatbestand eines Delikts des StGB oder des Nebenstrafrechts (VG, PornG usw) erfüllt. In erster Linie kommt eine Strafbarkeit des **Urhebers** in Betracht, also desjenigen, der die rechtswidrigen Inhalte im Internet (über einen Provider) verbreitet hat; dies kann der Verfasser, Autor, Fotograf usw sein oder derjenige, der die Inhalte des Urhebers im Internet zugänglich macht (zB jemand bietet Adolf Hitlers „Mein Kampf" auf seiner Homepage zum downloaden an). Die wichtigsten einschlägigen Strafbestimmungen für den Urheber rechtsextremer Inhalte finden sich unter den strafbaren Handlungen gegen den öffentlichen Frieden im StGB (s II.A.) sowie im VG (s II.B.). Kritische, journalistische oder seriöse wissenschaftliche Auseinandersetzungen mit dem Nationalsozialismus sind selbstverständlich straffrei.

Neben dem Urheber ist auch der **„Linksetzer"** von Bedeutung (s IV.), also derjenige, der via Hypertext[25]) auf die Seiten eines Urhebers verweist und damit die Verbreitung der dortigen Inhalte fördert. Von geringerer praktischer Bedeutung sind die **Moderatoren** insb von Diskussionsforen, Newsgroups oder Mailing-Lists, die darüber entscheiden, welche Inhalte publiziert oder versandt werden; sie sind gleich wie die Urheber zu behandeln[26]).

Vom Urheber zu unterscheiden ist jene Person, die für die Veröffentlichung der Inhalte verantwortlich ist und (idR gegen Entgelt) die technischen Einrichtungen dafür bereitstellt; der sog Internetservice-Provider oder kurz: **Provider.**

Man unterscheidet folgende Provider-Arten: **Network-Provider** (Netzwerk-Betreiber) oder „Carrier" stellen die Infrastruktur wie zB Telefonleitungen oder Kabelverbindungen zwischen Konsumenten und Providern zur Verfügung. **Access-Provider** vermitteln den Zugang zum Internet (zB *Jet2Web* oder *Chello*). **Host-Provider** stellen einem Urheber Speicherplatz für eine Website (Homepage) oder Beiträge (zB Leserbriefe) auf ihrem Web-Server zur Verfügung[27]); oder sie ermöglichen den Urhebern, ihre Information auf seinem Netz-Dienst einzugeben (zB in einem Diskussions- oder „Leserbrief-Forum" oder in einem „Gästebuch"). Provider, die neben fremden auch eigene Inhalte anbieten **(Content-Provider)**, gelten insoweit als Urheber. In der Praxis treten meistens Mischformen auf: So bieten zB Provider wie *CompuServe* oder *America Online* ihren Kunden neben Internetzugang und Speicherplatz auch Services wie zB Mailing-Lists, Newsgroups, Diskussionsforen, Informationen etc an. Reine Access-Provider sind selten[28]). Je

---

[19]) Ein Server ist – vereinfacht gesagt – ein vernetzter Computer, auf dem Daten (wie zB Homepages) gespeichert werden können. Jeder Internet-Dienst besteht grundsätzlich aus einem Server, der an das Internet angebunden ist. Dieser hat ein oder mehrere eindeutig zugewiesene Domain- und IP-Adressen, die ihn unverwechselbar machen. Im Prinzip kann jeder mit dem Internet verbundene PC auch als Server verwendet werden.

[20]) *Mayer-Schönberger,* Das Recht am Info-Highway, 96f und 107f; *Holznagel/Kussel,* MMR 2001, 351.

[21]) *Bremer,* Strafbare Internet-Inhalte in Internationaler Hinsicht (2001) 209f.

[22]) *Geisler,* Rechtsextremismus via Computer in Bundesministerium für Unterricht und Kunst/Dokumentationsarchiv des österreichischen Widerstandes (Hrsg), Amoklauf gegen die Wirklichkeit. NS-Verbrechen und revisionistische Geschichtsschreibung (1992) 107ff.

[23]) Es ist ja modern geworden, den Anbietern dadurch das Handwerk zu legen, dass man die Nachfrager bestraft, wie dies zB im Drogenstrafrecht durch die Pönalisierung des Erwerbs oder Besitzes von Suchtgift (§ 27 Abs 1 SMG) geschehen ist.

[24]) BGBl I 2001/152.

[25]) Hypertext ist eine Methode zur Präsentation und Vernetzung von Information. Bestimmte hervorgehobene Worte (meist farblich abgehoben und/oder unterstrichen) oder auch Grafiken enthalten eine Verbindung (Link, auch Hyperlink) zu einem anderen Inhalt (Text, Bild, Audio- oder Videodatei). Bei Aktivieren (Anklicken mit der Maus) wird dieser auf dem Bildschirm angezeigt. Dabei ist es gleichgültig, ob sich der Inhalt, auf den verwiesen wird, auf demselben Computer befindet oder auf einem anderen vernetzten Computer.

[26]) *Freund,* Internetdelikte 71.

[27]) IdR schließt der Urheber zunächst mit dem Host-Provider einen Vertrag über die Gewährung von Speicherplatz (und damit verbundener Internetadresse); dann schaltet der Provider den Urheber frei oder gibt ihm ein Passwort, mit dem er zu seinem Speicherplatz gelangt; anschließend kann der Urheber von seinem PC aus seine Dateien (Homepage) via *File-Transfer* (FN 138) auf den Speicherplatz laden (und in der Folge nach Belieben verändern).

[28]) *Stabentheiner,* Straf- und zivillegislativer Handlungsbedarf durch Datenhighway und Internet? ecolex 1996, 748 (750f). Nach *Schmölzer/Mayer-Schönberger* (Das Telekommunikationsgesetz 1997, ÖJZ 1998, 378, 383) existieren in Österreich praktisch keine reinen Access-Provider,

nach Art des Providers differieren auch die Haftungsvoraussetzungen. Keine Haftung trifft jedenfalls die reinen Network-Provider: Ihnen kann keine strafrechtliche Verantwortung für die Inhalte aufgetragen werden, da sie nur die reine Infrastruktur (Datenhighway) zur Verfügung stellen. Zum Haftungsumfang der anderen Provider s III.B.

Vom Urheber und Provider ist schließlich der (bloße), **Konsument** oder „Surfer" zu unterscheiden, also derjenige, der die strafbaren Inhalte im Zug des Internet-Surfens lediglich liest, ansieht, anhört oder speichert. Diesen trifft – zumindest was das bloße Konsumieren (Lesen, Ansehen etc) krimineller Inhalte angeht – keine strafrechtliche Haftung (s unter VI.).

II. Haftung des Urhebers neonazistischer Inhalte

A. §§ 281 ff StGB

1. **§ 281 StGB** stellt die **Aufforderung zum** allgemeinen **Ungehorsam gegen ein Gesetz** unter Strafe; diese Aufforderung muss in einem Druckwerk, im Rundfunk oder so geschehen, dass sie einer **breiten Öffentlichkeit zugänglich** wird.

Das **Internet** gilt als breite Öffentlichkeit[29]). **„Zugänglichmachen"** im Internet bedeutet, dass der Konsument den betreffenden Inhalt abrufen und lesen kann[30]). Unter **„Aufforderung"** ist jede Äußerung zu verstehen, die nach dem Vorsatz des Täters unmittelbar die Wirkung haben soll, in einem anderen den Entschluss zur Begehung einer strafbaren Handlung zu wecken[31]). Bei der Aufforderung muss der Wille des Täters erkenntlich sein, von anderen ein Verhalten zu fordern[32]). Die Aufforderung muss sich an die Allgemeinheit (also nicht bloß an Einzelpersonen) richten[33]). Bloß „milieubedingte Unmutsäußerungen" fallen nicht unter diesen Tatbestand[34]). Der Täter fordert zum „allgemeinen" Ungehorsam auf, wenn er dazu auffordert, ein **bestimmtes Gesetz** oder einzelne Gesetzesbestimmungen allgemein und nicht nur für den Anlassfall zu ignorieren[35]); beispielsweise wenn er auf seiner Homepage dazu auffordert, das VG zu missachten.

2. Gem **§ 282 StGB** ist mit Freiheitsstrafe bis zu zwei Jahren zu bestrafen, wer in einem Druckwerk, im Rundfunk oder sonst auf eine Weise, dass es einer breiten Öffentlichkeit zugänglich wird, **zu einer mit Strafe bedrohten Handlung auffordert,** soweit er nicht als an dieser Handlung Beteiligter (§ 12) mit strengerer Strafe bedroht ist (Abs 1). Ebenso ist zu bestrafen, wer auf die im Abs 1 bezeichnete Weise eine vorsätzlich begangene, mit einer ein Jahr übersteigenden Freiheitsstrafe bedrohte Handlung in einer Art gutheißt, die geeignet ist, das allgemeine Rechtsempfinden zu empören oder zur Begehung einer solchen Handlung aufzureizen (Abs 2).

Zum „Zugänglichmachen" und „Auffordern" s bereits oben unter 1. Das Auffordern bezieht sich auf eine gerichtlich strafbare Handlung, zB „Zündet Asylantenheime an!": Wer, wo, wann, welches Heim anzünden soll, ist für § 282 belanglos. Sobald die Tat aber individuell konkretisiert ist, liegt (versuchte) **Bestimmungstäterschaft** (§ 12 zweiter Fall StGB) vor, und der Täter ist nach dem entsprechenden Delikt zu verurteilen. Dabei wird man verlangen müssen, dass der Täter individuell bestimmte Personen zur Brandstiftung an einem bestimmten Objekt auffordert. Die an Internetbenützer gerichtete Aufforderung „Tötet XY" ist keine Bestimmung zum Mord, wenn noch gar nicht feststeht, wer die Tat ausführen soll[36]). **Gutheißen** (§ 282 Abs 2) bedeutet als rühmlich und nachahmenswert hinstellen, ausdrücklich billigen oder als positiv bewerten[37]). Das Gutheißen muss nur **geeignet** sein, das allgemeine Rechtsempfinden zu empören oder andere zur Begehung zu einer solchen Tat aufzureizen.

3. Das abstrakte Gefährdungsdelikt[38]) des **§ 283 Abs 1 StGB (Verhetzung)** pönalisiert ua die öffentliche Aufforderung oder Aufreizung zu einer feindseligen Handlung gegen eine einer Rasse, einem Volk(-sstamm) oder einem Staat zugehörigen Gruppe; das Auffordern oder Aufreizen muss dabei **geeignet sein,** die öffentliche Ordnung zu gefährden. Ebenso ist nach dem schlichten Tätigkeitsdelikt[38] des Abs 2 zu bestrafen, wer öffentlich gegen eine der in Abs 1 genannten Gruppen hetzt oder sie in einer die Menschenwürde verletzenden Weise beschimpft oder verächtlich zu machen sucht.

Rasse ist eine Menschengruppe, die bestimmte körperliche Merkmale zu anderen Gruppen aufweist (zB dunklere Hautfarbe); **Volk** ist im ethnischen Sinn (also unabhängig von Staatsgrenzen) zu verstehen; **Volksstamm** ist eine Minderheit der Bevölkerung[39]); **„Aufreizen"** ist ein leidenschaftliches auffordern[40]); **Beschimpfen** ist eine derbe Kundgebung von Missachtung; **verächtlich macht,** wer den anderen als der Achtung seiner Menschenwürde als unwert oder unwürdig hinstellt[41]). **In einer die Menschenwürde verachtenden Weise** werden Angehörige einer Gruppe beschimpft oder verächtlich gemacht, wenn ihnen das Lebensrecht abgesprochen oder sie als minderwertig dargestellt werden[42]); also zB die jüdische Bevölkerung mit Ausdrücken wie „Brut", „Saujuden" oder „Judenschweine"[43]) beschimpft wird; oder die Gruppe als eine solche, die vergast, vernichtet oder ausgetilgt werden soll, bezeichnet wird[44]). Es muss sich für die Tatbestandsmäßigkeit immer um **inländische Personengruppen** handeln, die durch ihre Zugehörigkeit zu einem Staat oder einem Volk bestimmt sind[45]). Die Hetze gegen „Ausländer", oder „Asylanten" im Allgemeinen ist daher nicht tatbildlich[46]); auch Hetze gegen politische (zB Parteien) oder weltanschauliche Gruppen fallen nicht unter § 283[47]). Wird gegen einzelne, individuell bestimmte Personen gehetzt, aufgereizt oder werden diese beschimpft, macht sich der Täter nach § 111 StGB (Üble Nachrede) oder § 115 StGB (Beleidigung) strafbar. Unter **feindselige Handlungen** fallen alle qualifizierten Diskriminierungen, die über jene Diskriminierungen hinausgehen, welche von der Verwaltungsstrafbestimmung des Art IX Abs 1 Z 3 EGVG erfasst sind[48]). Das **Internet** gilt als öffentlich[49]). Öf-

---

da jeder Zugangsvermittler auch Services wie Mail oder Newsgroups betreibt.

[29]) *Mayerhofer,* StGB[5] § 281 Anm 5; *Steininger* in WK[2] § 281 Rz 7.

[30]) *Auer/Loimer,* ÖJZ 1997, 618 zum Begriff des „Zugänglichmachens" des § 207a StGB.

[31]) EBRV 1971, 425.

[32]) *Steininger* in WK[2] § 281 Rz 2.

[33]) *Steininger* in WK[2] § 281 Rz 3.

[34]) *Lendl,* § 281 StGB: Ein bisher wenig beachteter Tatbestand, ÖJZ 1997, 551.

[35]) *Bertel/Schwaighofer,* BT II[4] § 281 Rz 1.

[36]) *Kienapfel/Höpfel,* AT[9], 216; aM *Fuchs* AT[4], 281.

[37]) EBRV 1971, 426.

[38]) *Steininger* in WK[2] § 283 Rz 5.

[39]) *Hinterhofer* BT II[2], 201 f; eingehend zum Minderheitenbegriff zB *Pernthaler/Ebensperger,* Minderheiten im Geltungsbereich der Alpenkonvention, Europa Ethnica 2000, 117 (119 ff).

[40]) *Bertel/Schwaighofer,* BT II[4] § 283 Rz 3. Zum Begriff des „Aufforderns" s unter II.A.1.

[41]) *Leukauf/Steininger,* StGB[3] § 283 Rz 6.

[42]) EBRV 1971, 427.

[43]) *Mayerhofer,* StGB[5] § 283 Anm 6.

[44]) EVBR 1971, 427.

[45]) *Hinterhofer* BT II[2], 202; *ders* in *Triffterer* StGB-Komm § 283 Rz 13.

[46]) *Bertel/Schwaighofer,* BT II[4] § 283 Rz 2; vgl dagegen den Verhetzungstatbestand des § 130 Abs 1 dStGB: Dort ist weitergehend als in Österreich die Diskriminierung von „Teilen der Bevölkerung" pönalisiert. Dieser Begriff umfasst alle Personenmehrheiten, die auf Grund gemeinsamer äußerer und innerer Merkmale als unterscheidbarer Teil von der Gesamtheit der Bevölkerung abgrenzbar ist (*Tröndle/Fischer,* StGB[50] § 130 Rz 2), somit auch alle im Inland lebenden „Ausländer", „Asylanten" etc. ME sollte § 283 der deutschen Regelung angeglichen werden, weil es keinen gesetzlichen Unterschied machen darf, ob jemand gegen im Inland lebende Juden oder Asylanten hetzt.

[47]) *Steininger* in WK[2] § 283 Rz 1.

[48]) *Hinterhofer* in *Triffterer,* StGB-Komm § 283 Rz 20.

[49]) *Mayerhofer,* StGB[5] § 283 Anm 7.

fentliche Ordnung iSd § 283 ist nur die öffentliche Ordnung Österreichs[50]). Ist die Tat nach den §§ 3d, 3g oder 3h VG strafbar, scheidet eine Verurteilung (auch) nach § 283 StGB wegen Spezialität aus[51]).

4. Da das Gesetz für die **Tathandlungen der §§ 281 bis 283 StGB** (Hetzen etc) **keine bestimmte Form** verlangt, müssen diese für die Tatbestandsmäßigkeit nicht in Schriftform erfolgen, sondern sie können sich auch aus Bildern, Filmen, Musikdateien, Spielen etc ergeben; der Täter bietet zB im Internet „Nazi-Rock" mit antisemitischen Tiraden als mp3-Dateien zum downloaden an (§ 283 StGB).

B. Strafbarkeit nach dem VG[52])

1. Nach **§ 3h VG** wird mit Freiheitsstrafe von einem bis zu zehn Jahren bestraft, wer in einem Druckwerk, im Rundfunk oder in einem anderen Medium oder wer sonst öffentlich auf eine Weise, dass es vielen Menschen zugänglich wird, den nationalsozialistischen Völkermord oder andere Verbrechen gegen die Menschlichkeit leugnet, gröblich verharmlost, gutheißt oder zu rechtfertigen sucht **(„Auschwitz-Lüge").**

Die im Internet öffentlich zugänglichen Bereiche (Homepages, Newsgroups usw) sind als **„Medium"** iSd § 3h VG anzusehen[53]). Für die **Öffentlichkeit** ist es erforderlich, dass die Inhalte so eingespeist werden, dass sie (sei es auf einer Homepage, in einer Newsgroup, in einem Chat etc) von einem „größeren Personenkreis", also ab zehn Personen[54]), wahrgenommen werden können. „Gesperrte" Seiten, zu denen nur der Urheber oder ein sehr kleiner Personenkreis (insb mit Passwort) Zugang hat, sind demnach nicht öffentlich; gleiches gilt für e-mails (an weniger als zehn Personen). Der nationalsozialistische **Völkermord** bestand in der planmäßigen Vernichtung von Menschen wegen ihrer Zugehörigkeit zu einer Rasse, einem Volk oder Volksstamm oder wegen ihrer politischen oder religiösen Überzeugung, insb in Vernichtungs- oder Konzentrationslagern[55]). Dieser Völkermord ist verfassungsrechtlich außer Streit gestellt, er braucht also nicht mehr bewiesen werden[56]). **„Leugnen"** bedeutet, schlechthin und im Kern in Abrede stellen[57]). Tatbildmäßig gem § 3h VG handelt also, wer zB im Internet den Holocaust oder die Existenz von Gaskammern im Nationalsozialismus bestreitet. Auf der **inneren Tatseite** muss es dem Täter bei seinen Behauptungen um das direkte oder indirekte Leugnen, Gutheißen oder grobe Verniedlichen des nationalsozialistischen Massenmordes gehen[58]). In **Deutschland** ist die „Auschwitzlüge" in § 130 Abs 3 dStGB geregelt[59]).

2. Auch **§ 3d VG** könnte einschlägig sein: Wer öffentlich oder vor mehreren Leuten, in Druckwerken, **verbreiteten Schriften** oder bildlichen Darstellungen zu einer der nach § 1 (Neubildung der NSDAP) oder § 3 (Betätigung für die NSDAP oder ihre Ziele) verbotenen Handlungen auffordert, aneifert oder zu verleiten versucht, insb zu diesem Zweck die **Ziele der NSDAP,** ihrer Einrichtungen oder Maßnahmen **verherrlicht** oder anpreist, ist, sofern die Tat nicht schon durch einen anderen Tatbestand mit schwererer Strafe bedroht ist, mit Freiheitsstrafe von fünf bis zu zehn Jahren, bei besonderer Gefährlichkeit des Täters oder der Betätigung mit bis zu zwanzig Jahren bedroht.

Durch den Hinweis in § 3d auf § 3 VG gilt die Strafdrohung des § 3d für jede öffentliche Aufforderung zur nationalsozialistischen Wiederbetätigung[60]). Die Begehungsweise „in einem Medium" wie bei § 3h fehlt bei § 3d allerdings. So ist fraglich, ob Wiederbetätigung im Internet unter § 3d subsumiert werden kann, ob also mit **„Schriften"** auch Inhalte im Internet gemeint sind. Manche wollen auch „digitale" Schriften einbeziehen[61]). Aber an „digitale" Schriften dachte der Verfassungsgesetzgeber 1945 wohl kaum. Die nationalsozialistische Wiederbetätigung im Internet bleibt darum nicht straflos: Sie wird auf „andere Weise" als durch Schriften begangen und fällt unter den Auffangtatbestand des § 3g VG:

3. Wer sich **auf andere Weise** als in den §§ 3a–3f VG **im nationalsozialistischen Sinn betätigt,** ist, sofern die Tat nach einer anderen Bestimmung nicht strenger bestraft wird, nach **§ 3g VG** mit Freiheitsstrafe von einem bis zu zehn Jahren, bei besonderer Gefährlichkeit des Täters oder der Betätigung bis zu 20 Jahren zu bestrafen.

Nach *Platzgummer* fällt unter (Wieder-)**Betätigung** im nationalsozialistischen Sinn jedes Verhalten, das darauf abzielt, in Österreich wieder ein Naziregime zu installieren[62]). Laut OGH fällt darunter die völlig einseitige, propagandistische, vorteilhafte Darstellung nationalsozialistischer Ziele[63]); also zB eine unverkennbare Glorifizierung Adolf Hitlers und eine deutlich erkennbare Gutheißung seiner Lebensaufgabe[64]), die Bezeichnung des Widerstands gegen das NS-Regime als Verrat[65]) oder die Verherrlichung des Anschlusses Österreichs an Nazideutschland im Jahre 1938[66]). § 3g VG sieht keine bestimmten Begehungsweisen vor; es genügt die **nationalsozialistische Wiederbetätigung in irgendeiner Form** (also auch via Internet).

C. Exkurs: Medienrecht

Die im **Internet** öffentlich zugänglichen Bereiche (Homepages, Newsgroups, Internetzeitschriften usw) sind **als „Medium" iSd MedG** anzusehen: Sie fallen unter die Legaldefinition des § 1 Abs 1 Z 1 MedG[67]). Äußerungs- und Verbreitungsdelikte nach dem StGB (zB §§ 111, 115, 281, 282, 283), VG, PornG etc sind **Medieninhaltsdelikte** iSd § 1 Abs 1 Z 12 MedG[68]). Die Qualifikation einer Tat als Medieninhaltsdelikt hat va **prozessuale Folgen:** So kann zB eine Urteilsveröffentlichung gem § 34 MedG begehrt werden und die gerichtliche Zuständigkeit richtet sich nach

---

[50]) *Steininger* in WK² § 83 Rz 15.

[51]) SSt 59/91, 60/4; *Hinterhofer* in *Triffterer,* StGB-Komm § 283 Rz 34; *Bertel/Schwaighofer,* BT II⁴ § 283 Rz 9.

[52]) Verfassungsgesetz vom 8. 5. 1945, StGBl 13 über das Verbot der NSDAP, zuletzt idF BGBl 1992/148. Eingehend dazu *Bertel,* Die Betätigung im nationalsozialistischen Sinn, in *Platzgummer*-FS 1995, 119; *Platzgummer,* Die strafrechtliche Bekämpfung des Neonazismus in Österreich, ÖJZ 1994, 753.

[53]) *Stabentheiner,* ecolex 1996, 750.

[54]) *Leukauf/Steininger* (StGB³ § 69 Rz 3) sprechen von „etwa ab zehn Menschen".

[55]) *Mayerhofer/Rieder* Das österreichische Strafrecht, 3. Teil: Nebenstrafrecht⁴ (1997) § 3h VG Anm 3; zum Begriff „Verbrechen gegen die die Menschlichkeit" s ebenfalls dort.

[56]) *Platzgummer,* ÖJZ 1994, 762 unter Hinweis auf EvBl 1994/54.

[57]) 387 BlgNR 18. GP 4; RZ 1997/4; *Platzgummer,* ÖJZ 1994, 762.

[58]) RZ 1997/4.

[59]) § 130 Abs 3 dStGB lautet: „Mit Freiheitsstrafe bis zu fünf Jahren oder mit Geldstrafe wird bestraft, wer eine unter der Herrschaft des Nationalsozialismus begangene Handlung der in § 220a Abs 1 bezeichneten Weise, die geeignet ist, den öffentlichen Frieden zu stören, öffentlich oder in einer Versammlung billigt, leugnet oder verharmlost."

[60]) *Platzgummer,* ÖJZ 1998, 759.

[61]) ZB *Stabentheiner,* ecolex 1996, 750; *Freund,* Internetdelikte 24ff.

[62]) *Platzgummer,* ÖJZ 1998, 760.

[63]) JBl 1993, 598.

[64]) EvBl 1969/230.

[65]) EvBl 1987/40.

[66]) EvBl 1979/154.

[67]) *Brandstetter/Schmid,* Mediengesetz. Kommentar² (1999) § 1 Rz 4, 16, 19; *Schmölzer,* Internet und Strafrecht, in StPG 25, 157.

[68]) *Brandstetter/Schmid,* MedienG² § 28 Rz 8; *Stabentheiner,* ecolex 1996, 750; OLG Wien 26. 5. 2000, 18 Bs 143/00, MR 2000, 140.

den §§ 40f MedG, die in diesem Fall den Bestimmungen der 51ff StPO vorgehen. **Musikbörsen im Internet** (zB „Napster") gelten nach einer Entscheidung des OLG Wien[69]) medienrechtlich als Rundfunksendung; werden zB Musikdateien („mp3s") mit hetzerischem Inhalt (§ 283 StGB) angeboten, ist im Regelfall das LGSt Wien zuständig (§ 41 Abs 2, 2. Satz MedG).

D. Verwaltungsstrafrecht

1. Formell **subsidiär zum VG** gilt die Verwaltungsstrafbestimmung des **Art IX Abs 1 Z 4 EGVG:** Wer nationalsozialistisches Gedankengut iSd VG verbreitet, begeht, wenn die Tat nicht gerichtlich strafbar ist, eine Verwaltungsübertretung und ist mit einer Geldstrafe bis zu 2.180 EUR und mit dem Verfall der Gegenstände, mit denen die strafbare Handlung begangen wurde, zu bestrafen. Auch der Versuch dieses Delikts ist ausdrücklich strafbar[70]).

Ein Inhalt ist im Internet **verbreitet,** wenn die Datei auf dem Rechner des Konsumenten angekommen ist; dabei ist es unerheblich, ob dieser die Möglichkeit des Zugriffs auf die Daten genutzt oder ob der Urheber die Daten übermittelt hat[71]). Für die Strafbarkeit des unmittelbaren Täters genügt im Gegensatz zum VG bereits Fahrlässigkeit (§ 5 Abs 1 VStG); andere Beteiligte (zB Provider als Beihelfer) haften dagegen nur bei Vorsatz (§ 7 VStG). Da aber an sich jede Wiederbetätigung unter den Auffangtatbestand des § 3g VG fällt, wäre Art IX Abs 1 Z 4 EGVG praktisch unanwendbar. Der VfGH hat daher klargestellt, dass die Verwaltungsstrafbestimmung dann eingreift, wenn der Täter ohne **Wiederbetätigungsvorsatz,** also ohne den Vorsatz, in Österreich wieder ein Naziregime zu installieren, handelt, aber die Tat als öffentliches Ärgernis erregender Unfug empfunden wird[72]). Wer also mit Nazipropaganda **lediglich provozieren** will, fällt nicht unter das VG, sondern unter Art IX Abs 1 Z 4 EGVG[73]).

2. Einschlägige Verwaltungsstraftatbestände finden sich auch im **AbzeichenG**[74]): Gem § 1 Abs 1 leg cit dürfen ua **Abzeichen** einer in Österreich verbotenen Organisation (wie der NSDAP) **öffentlich nicht dargestellt oder verbreitet** werden. Als Abzeichen sind auch Embleme, Symbole und Kennzeichen anzusehen. Der Strafrahmen reicht bis zu 726 EUR Geldstrafe und/oder einem Monat Arrest (§ 3 Abs 1 AbzeichenG). Diesen Straftatbestand erfüllt, wer zB **Hakenkreuzbilder** auf seiner Website platziert.

3. Verwaltungsstrafbestimmungen (ua) für den Urheber finden sich schließlich auch im Telekommunikationsgesetz (§§ 104 Abs 1 iVm § 75 TKG). Demnach droht bei missbräuchlicher Verwendung von Endgeräten (zB PC, Web-Server[75])) im Fall der Übermittlung gesetzwidriger Inhalte eine Verwaltungsstrafe bis 3.633 EUR. „Missbräuchlich" und damit strafbar ist die Übermittlung gesetzwidriger, somit auch neonazistischer Inhalte, sofern die Tat nicht ohnehin gerichtlich strafbar ist (§ 104 Abs 4 TKG).

[69]) OLG Wien 18. 5. 2001, 21 Ns 97/01.

[70]) Eingehend zu dieser Bestimmung *Merli,* Das Verbot der Verbreitung nationalsozialistischen Gedankenguts im EGVG, JBl 1986, 767.

[71]) BGH 27. 6. 2001, 1 StR 66/01, NStZ 2001, 596.

[72]) VfSlg 12.002/1989 = ÖJZ 1990, 499.

[73]) *Bertel,* in *Platzgummer*-FS 123f.

[74]) Bundesgesetz mit dem bestimmte Abzeichen verboten werden, BGBl 1960/84 idF BGBl 1980/117.

[75]) „Endgerät" ist eine Einrichtung, die unmittelbar an die Netzabschlusspunkte eines öffentlichen Telekommunikationsnetzes angeschlossen werden soll oder die mit einem öffentlichen Telekommunikationsnetz zusammenarbeiten und dabei unmittelbar oder mittelbar an die Netzabschlusspunkte eines öffentlichen Telekommunikationsnetzes angeschlossen werden soll (§ 3 Z 2 TKG). Darunter fallen somit auch die Web-Server eines Providers oder ans Internet angeschlossene PCs (von Konsumenten oder Urhebern).

III. Providerhaftung

A. Allgemeines

Zu den einzelnen Arten der Provider s bereits I.B. Die Providerhaftung bestimmt sich nach denselben Delikten wie für den Urheber. In Betracht kommt eine Haftung des Providers wegen unmittelbarer (Mit-)Täterschaft oder wegen Beitrags (§ 12 3. Fall StGB)[76]) zu den einschlägigen Bestimmungen im StGB, VG etc. IdR wird ein Beitrag des Providers vorliegen, da der Urheber nach Erhalt seines Speicherplatzes (mittels *File-Transfer*) seine Inhalte selbst ins Netz stellen kann. Der Provider kann dem Urheber aktiv den Zugang zum Internet ermöglichen oder Speicherplatz zur Verfügung stellen (Tun) oder trotz Kenntnis des Seiteninhalts die betreffenden Informationen nicht entfernen oder sperren (Strafbarkeit durch Unterlassen – § 2 StGB[77])). Für die Strafbarkeit durch **Unterlassen** müssen aber noch weitere Voraussetzungen[78]) vorliegen: Der Provider muss auch die tatsächliche (technische) **Möglichkeit** besitzen, die Seite zu sperren oder zu löschen. Befindet sich zB eine Kopie der Seite auf einem anderen Server, zu dem der Provider keinen Zugang hat, so muss er für eine Haftungsbefreiung nur die Seite auf seinem Server sperren/löschen. Weiters muss der Provider Garant sein; in Betracht kommt eine **Garantenstellung auf Grund der §§ 13ff ECG**[79]) (dazu gleich unten); so lässt sich zB aus § 16 ECG die Verpflichtung des Host-Providers ableiten, bei Kenntnis eines (von ihm gespeicherten) rechtswidrigen Inhalts diesen unverzüglich zu löschen oder zu sperren. Hat sich der Provider vertraglich den **ISPA-Richtlinien** (s VIII.A.) unterworfen, so besteht auch diesbezüglich eine Garantenstellung auf Grund freiwilliger Pflichtübernahme. **Gleichwertigkeit** der Unterlassung des Nicht-Sperrens einer Seite gegenüber einer aktiven Zugangs- oder Speichervermittlung liegt vor, wenn der Provider gezielt unterlässt[80]), dh, wenn es ihm darauf ankommt, dass die kriminellen Inhalte einem Dritten zugänglich sind. Dass er sie nur aus Überlastung oder Bequemlichkeit nicht löscht/sperrt, genügt dagegen nicht. Das Vorgehen des Providers ist schließlich auch (quasi-)**kausal** für die Publikation der Inhalte im Internet: Hätte der (Host-)Provider dem Urheber nicht Speicherplatz für seine Seiten im Internet überlassen bzw hätte er die Seiten mit den kriminellen Inhalten gesperrt/gelöscht, wäre eine (weitere) Verbreitung/Veröffentlichung im Internet sehr wahrscheinlich nicht eingetreten.

Neben den unechten Unterlassungsdelikten könnte man auch die Anwendung des echten Unterlassungsdelikts des

[76]) Zur Abgrenzung zwischen unmittelbarer Mittäterschaft und Beitragstäterschaft s *Kienapfel/Höpfel,* AT[9] E 3 Rz 7ff. Auf Grund des österr Einheitstätersystems ist diese Abgrenzung von geringer praktischer Bedeutung; s aber FN 77.

[77]) Eingehend zur Strafbarkeit des Providers durch Unterlassen *Auer/Loimer,* ÖJZ 1997, 618ff. Da die Äußerungs- und Verbreitungsdelikte als schlichte Tätigkeitsdelikte anzusehen sind (s VII.A.) kommt für sie nach hM (s *Kienapfel* AT[9] Z 28 Rz 19 mwN) nur ein Beitrag durch Unterlassen, nicht aber unmittelbare Täterschaft durch Unterlassen in Frage.

[78]) Siehe eingehend dazu zB *Kienapfel/Höpfel,* AT[9] Z 29.

[79]) Eine Garantenstellung auf Grund von § 75 Abs 2 TKG, der die Provider verpflichtet, geeigneten Maßnahmen zu treffen, um eine missbräuchliche Verwendung von Endgeräten auszuschließen, kommt auf Grund des § 18 Abs 1 ECG nicht (mehr) in Betracht: Demnach besteht für die Provider keine Verpflichtung, die von ihnen gespeicherten, übermittelten oder zugänglich gemachten Informationen allgemein zu überwachen oder von sich aus nach Umständen zu forschen, die auf rechtswidrige Tätigkeiten hinweisen.

[80]) Vgl EvBl 2000/101.

§ 286 StGB (Unterlassung der Verhinderung einer mit Strafe bedrohten Handlung) in Erwägung ziehen: § 286 begründet aber bei abstrakten Gefährdungsdelikten (und als solche sind die Äußerungs- und Verbreitungsdelikte anzusehen) keine Verhinderungspflicht (s unter VI.).

Der **Vorsatz** des Providers muss sich (im Fall der gerichtlichen Strafbarkeit) auf eine/n bestimmte Tat/bestimmten Inhalt beziehen; der Vorsatz darauf, dass es im Internet zahlreiche Seiten mit kriminellem Inhalt gibt und dass solche auch auf seinem Server existieren könnten, genügt nicht; sein Vorsatz muss sich vielmehr darauf beziehen, dass ein bestimmter Urheber auf seinem Server eine Seite mit einem bestimmten kriminellen Inhalt gespeichert hat. Das E-Commerce-Gesetz verlangt für den Host-Provider hinsichtlich des rechtswidrigen Inhalts **tatsächliche Kenntnis** (s III.B.4). Für die Verwaltungsstraftatbestände genügt bereits **Fahrlässigkeit** (§ 5 Abs 1 VStG), sofern der Provider als unmittelbarer (Mit-)Täter und nicht als Beihelfer haftet (§ 7 VStG).

B. Haftungsausschluss nach dem ECG

1. Allgemeines

Das E-Commerce-Gesetz[81]) (ECG) dient in erster Linie der Umsetzung der E-Commerce-Richtlinie der EU (ECRL)[82]), geht aber zT (wie zB bei der „Linkhaftung") darüber hinaus. Es sieht insb Bestimmungen über den Ausschluss der Verantwortlichkeit bestimmter Provider vor: Access- und Host-Provider sollen unter bestimmten Voraussetzungen von der zivil- und strafrechtlichen Haftung für kriminelle Inhalte freigestellt werden. Das Gesetz enthält ferner auch Regelungen über die Haftung der Betreiber von Suchmaschinen und von Linksetzern. Es trat am 1. 1. 2002 in Kraft (§ 30 ECG). Die strafrechtlich relevanten Bestimmungen sind im 5. Abschnitt unter **„Verantwortlichkeit von Diensteanbietern"** (§§ 13ff ECG) geregelt. Diese setzen die Art 12 bis 15 ECRL um.

Diensteanbieter ist eine natürliche oder juristische[83]) Person, die einen **Dienst der Informationsgesellschaft** bereitstellt (§ 3 Z 2 ECG). Unter einem solchen Dienst versteht das Gesetz einen „in der Regel gegen Entgelt elektronisch im Fernabsatz auf individuellen Abruf des Empfängers bereitgestellter Dienst (§ 1 Abs 1 Z 2 Notifikationsgesetz 1999), insbesondere der Online-Vertrieb von Waren und Dienstleistungen, Online-Informationsangebote, die Online-Werbung, elektronische Suchmaschinen und Datenabfragemöglichkeiten sowie Dienste, die Informationen über ein elektronisches Netz übermitteln, die den Zugang zu einem solchen vermitteln oder die Informationen eines Nutzers speichern" (§ 3 Z 1 ECG). **Access- und Hostprovider** fallen jedenfalls klar unter die Diensteanbieter („Dienste, die den Zugang zu einem elektronischen Netz vermitteln oder die Informationen eines Nutzers speichern"); ebenso gelten für **private Linksetzer** (die neben Links auch Informationen anbieten) die Regelungen des 5. Abschnitts (insb § 17 ECG): Da § 3 Z 1 ECG von „Online-Informationsangeboten" spricht, fallen unter den Begriff des Diensteanbieters alle Personen, die Informationen in irgendeiner Form anbieten; und gem § 19 Abs 2 ECG sind – im Gegensatz zur ECRL[84]) – die Regeln des 5. Abschnitts **auch** auf Anbieter anzuwenden, die **unentgeltlich** (also ohne Ertrags- und Gewinnabsicht) Dienste bereitstellen.

Die Haftungsprivilegien gelten nicht nur für die Diensteanbieter, sondern auch für deren **Organe und Bedienstete**[85]), außer wenn es sich bei dem Organ oder Bediensteten um den Urheber der rechtswidrigen Information handelt (vgl § 14 Abs 2, § 16 Abs 2 und § 17 Abs 2 ECG).

Das ECG stellt den Diensteanbietern die sog **„Nutzer"** gegenüber, wobei unter letzteren nach der in der vorliegenden Untersuchung verwendeten Terminologie teils die Urheber, teils die Konsumenten krimineller Inhalte verstanden werden: § 3 Z 4 ECG definiert den Nutzer als „eine natürliche oder juristische Person oder sonst rechtsfähige Einrichtung, die zu beruflichen oder sonstigen Zwecken einen Dienst der Informationsgesellschaft in Anspruch nimmt, insbesondere um Informationen zu erlangen [Konsument] oder Informationen zugänglich zu machen [Urheber]."

Die §§ 13ff ECG regeln die **„Verantwortlichkeit"** von Diensteanbietern; diese umfasst querschnittsmäßig sowohl die schadenersatzrechtliche als auch die kriminal- und verwaltungsstrafrechtliche Haftung. Nur wenn keine Haftungsbefreiung nach dem ECG vorliegt, kommt eine Haftung nach dem materiellen Straf-, Zivil- und Verwaltungsstrafrecht in Betracht. Die §§ 13 bis 17 enthalten nach der RV Strafausschließungsgründe, schließen also bei Vorliegen eines tatbestandsmäßigen, rechtswidrigen und schuldhaften Verhalten die Strafbarkeit nach einem bestimmten Delikt des StGB oder des Nebenstrafrechts aus[86]). Dem ECG kommt somit eine Art **„Filterwirkung"** zu, es regelt die Voraussetzungen dafür, ob eine strafrechtliche Haftung (nach den materiellen Bestimmungen des StGB, VG usw) überhaupt möglich ist. Liegen die Haftungsbefreiungsvoraussetzungen nach dem ECG nicht vor, heißt das aber nicht, dass der Diensteanbieter automatisch haftet, sondern ist erst die Haftung nach den in Betracht kommenden jeweiligen Tatbeständen zu prüfen[87]).

Der in allen §§ des 5. Abschnitts ECG vorkommende Begriff der **„Information"** ist der ECRL entnommen und umfasst alle Inhalte (Texte, Bilder, etc), die im Rahmen des jeweiligen Dienstes übermittelt oder gespeichert werden. Der Ausschluss der strafrechtlichen Verantwortlichkeit bezieht sich immer nur auf **fremde** (also nicht vom Provider oder einer ihm unterstehenden Person stammende) Informationen; für eigene Inhalte haftet der Diensteanbieter als Urheber nach allgemeinen Regeln.

Gem § 18 ECG, der § 15 ECRL umsetzt, sind die Diensteanbieter der §§ 13 bis 17 ECG **nicht verpflichtet,** die von ihnen **gespeicherten oder übermittelten Informationen allgemein zu überwachen** oder von sich aus nach Umständen zu forschen, die auf eine rechtswidrige Tätigkeit hinweisen (Abs 1). Derartige Überwachungspflichten können den

[81]) Bundesgesetz, mit dem bestimmte rechtliche Aspekte des elektronischen Geschäfts- und Rechtsverkehrs geregelt werden, BGBl I 2001/152.

[82]) Richtlinie 2000/31/EG vom 8. 6. 2000 über bestimmte rechtliche Aspekte der Dienste der Informationsgesellschaft, insbesondere des Elektronischen Geschäftsverkehrs, im Binnenmarkt („Richtlinie über den Elektronischen Geschäftsverkehr"), ABl 2000 L 178, 1. Die Umsetzungsfrist endete mit 17. 1. 2002 (Art 22 ECRL).

[83]) Eine strafrechtliche Haftung kommt dzt nur für natürliche Personen in Betracht; vgl aber den Entw des BMJ über die Strafbarkeit juristischer Personen (eingehend dazu *Zeder,* Ein Strafrecht juristischer Personen: Grundzüge einer Regelung in Österreich, ÖJZ 2001, 630).

[84]) Dies ergibt sich aus dem Zusammenwirken von Art 1 Abs 1 ECRL und den Begriffsbestimmungen des Art 2c ECRL.

[85]) EBRV 817 BlgNR 21. GP Erläut 1 zu § 13.

[86]) EBRV 817 BlgNR 21. GP Erläut 1 zu § 13.

[87]) *Zankl,* E-Commerce-Gesetz in Sicht, AnwBl 2001, 459 (460).

Diensteanbietern auf Grund der Informationsfülle[88]) nicht zugemutet werden[89]). Sie können aber Mechanismen oder Instrumente (zB Filterprogramme) anwenden, um eine Speicherung und Übermittlung von rechtswidrigen Inhalten zu verhindern[90]).

Die Diensteanbieter der §§ 13 bis 16 ECG (also insb Access- und Host-Provider) haben auf Grund der **Anordnung eines dazu befugten inländischen Gerichts** diesem **alle Informationen zur Verfügung zu stellen,** anhand deren die **Nutzer** ihres Dienstes, mit denen sie Vereinbarungen über die Übermittlung oder Speicherung von Informationen abgeschlossen haben, zur Verhütung, Ermittlung, Aufklärung oder Verfolgung **ermittelt** werden können (§ 18 Abs 2 ECG). Die Herausgabe der Daten setzt voraus, dass der Diensteanbieter auch über die entsprechenden Informationen verfügt und dass das Gericht zu einer solchen Anordnung gesetzlich befugt ist[91]). Für eine solche gesetzliche Befugnis kommen insb § 89 TKG und die Bestimmungen der **§§ 149a ff StPO (Überwachung eines Fernmeldeverkehrs**[92]) in Betracht[93]). Eine Überwachung des Fernmeldeverkehrs ist unter den Voraussetzungen des § 149a StPO[94]) mit richterlichem Beschluss anzuordnen. Gem **§ 89 Abs 2 TKG** ist der **Provider** als Betreiber eines öffentlichen Telekommunikationsdienstes[95]) **verpflichtet, an der Überwachung** des Fernmeldeverkehrs nach den Bestimmungen der StPO im erforderlichen Ausmaß **mitzuwirken.** Der Provider ist aber nicht verpflichtet, seine Einrichtungen überwachungstauglich zu gestalten: Die kürzlich erlassene ÜberwachungsV (UVO; BGBl II 2001/418), die in § 3 eine derartige Verpflichtung vorsieht, richtet sich an Betreiber konzessionspflichtiger mobiler Sprachtelefondienste und anderer öffentlicher Mobilfunkdienste (§ 2 Abs 1 UVO iVm § 14 TKG), gilt also nicht für Diensteanbieter der §§ 13 bis 17 ECG. In § 19 Abs 1 ECG wird klargestellt, dass von den §§ 13 bis 18 ECG gesetzliche Vorschriften, nach denen ein Gericht oder eine Behörde dem Diensteanbieter die Unterlassung, Beseitigung oder Verhinderung einer Rechtsverletzung auftragen kann, unberührt bleiben. In der StPO befinden sich dzt aber noch keine gesetzlichen Grundlagen, denen zufolge ein Richter einem Provider die Löschung oder Sperrung von Internet-Inhalten vorschreiben könnte; solche Aufträge sind dzt nur nach dem Zivilrecht möglich. Allerdings kommt bei Nicht-Sperren von kriminellen Inhalten trotz Kenntnis eine Haftung des Providers durch Unterlassen (§ 2 StGB) in Betracht (s III.A. und III.B.4).

Öffentlich zugängliche Inhalte kann der Provider ohne behördliche Anordnung selbst überwachen. Nicht öffentlich zugängliche Informationen (E-mails) unterliegen aber auch für den Diensteanbieter dem Fernmeldegeheimnis (Art 10a StGG, Art 8 MRK). Das (bloße) Öffnen oder Lesen fremder e-mails ist nicht strafbar, da ein e-mail kein Schriftstück iSd § 118 StGB (Verletzung des Briefgeheimnisses) darstellt[96]) und § 119 StGB (Verletzung des Fernmeldegeheimnisses) das Anbringen, Benützen oder Empfangsbereitmachen einer (mechanischen[97])) Vorrichtung verlangt. Gerichtlich strafbar ist allerdings, wer einem Dritten Kenntnis von Inhalt fremder e-mails verschafft (§ 102 Abs 1 TKG).

2. Haftungsbefreiung bei Durchleitung (§ 13 ECG, Art 12 ECRL)

§ 13 ECG, der Art 12 ECRL entspricht, regelt den „Ausschluss der Verantwortlichkeit bei Durchleitung": Unter **Durchleitung** wird einerseits die **Zugangsvermittlung** zu einem Informationsnetz und andererseits die bloße **Datenübermittlung,** die sich aus der Übertragung von Informationen und der Vermittlung des Zugangs zu diesen zusammensetzt, verstanden (§ 13 Abs 1 ECG). Ein Diensteanbieter, der von einem Nutzer eingegebene Informationen in einem Kommunikationsnetz übermittelt oder den Zugang zu einem Kommunikationsnetz vermittelt (also insb ein reiner **Access-Provider**), ist für die Informationen **nicht verantwortlich, sofern** er die Übermittlung nicht veranlasst, den Empfänger der übermittelten Information nicht auswählt und die übermittelten Informationen weder auswählt noch verändert[98]) (Abs 1). Der Provider darf also – abgesehen von der bloßen Über- oder Vermittlung und der damit allenfalls einhergehenden kurzzeitigen Zwischenspeicherung der Informationen (§ 13 Abs 2) – **mit der übermittelten Information nicht in Verbindung** stehen bzw muss sie unverändert weitergeben[99]). Sobald er aber in einer der beschriebenen Weisen an der Übermittlung beteiligt ist, verliert er sein Haftungsprivileg. Die bloße Kenntnis (der Durchleitung) einer rechtswidrigen Information schadet aber dem Access-Provider im Gegensatz zum Host-Provider und Linksetzer nicht. Der Access-Provider haftet also nicht wenn er zB weiß, dass sich seine Kunden Kinderpornos oder neonazistische Inhalte ansehen.

3. Haftungsbefreiung beim Caching (§ 15 ECG, Art 13 ECRL)

Unter „Caching" wird das **automatische und zeitlich begrenzte Speichern** (auf sog „Proxy-Servern") verstanden; es wird verwendet, um den Nutzern einen schnelleren Zugang zu häufiger abgefragten Informationen zu verschaffen (vgl dagegen aber das Zwischenspeichern zur Informationsüber-

[88]) So fallen zB bei einem Access-Provider durchschnittlich pro Stunde 12 Gigabyte an Daten an (Tendenz steigend), was 5 Millionen Din-A4-Seiten entspricht; Berliner Erklärung gegen Netz des Hasses, www.heise.de/tp/deutsch/inhalt/te/8291/1.html (10. 9. 2001).

[89]) EBRV 817 BlgNR 21. GP Erläut 2 zu § 18.

[90]) EBRV 817 BlgNR 21. GP Erläut 2 zu § 18.

[91]) EBRV 817 BlgNR 21. GP Erläut 3 zu § 18.

[92]) Unter den Fernmeldeverkehr fallen neben Telefonaten und e-mails auch der Datenverkehr (*File-Transfer)* vom Nutzer zum Provider.

[93]) EBRV 817 BlgNR 21. GP Erläut 3 zu § 18.

[94]) Gem § 149a Abs 2 StPO ist eine Überwachung zulässig, wenn dadurch die Aufklärung einer mit mehr als sechsmonatiger Freiheitsstrafe bedrohten strafbaren Handlung gefördert werden kann und der Inhaber des Teilnehmeranschlusses (Provider) der Überwachung zustimmt (Z 1); oder die Überwachung zur Aufklärung einer vorsätzlich begangenen, mit mehr als einjähriger Freiheitsstrafe bedrohten strafbaren Handlung erforderlich scheint und der Inhaber selbst dringend verdächtig ist, die Tat begangen zu haben (Z 2 lit a) oder Gründe für die Annahme vorliegen, dass der dringend Tatverdächtige (Urheber) eine Verbindung mit dem Teilnehmeranschluss (des Providers) hergestellt hat oder herstellen wird (Z 2 lit b). Lit b liegt zB dann vor, wenn der Urheber seine Dateien (Homepage) via *File-Transfer* (dazu FN 138) an den Provider gesandt hat.

[95]) Ein Telekommunikationsdienst ist gem § 3 Z 14 TKG eine gewerbliche Dienstleistung, die in der Übertragung und/oder Weiterleitung von Signalen auf Telekommunikationsnetzen besteht (. . .).

[96]) *Lewisch* in WK² § 118 Rz 3.

[97]) *Leukauf/Steininger,* StGB³ § 119 Rz 10; aM wohl *Lewisch* in WK² § 119 Rz 4.

[98]) Eingriffe technischer Art, wie zB Verschlüsselung oder Datenkompressionen, die den Inhalt der Informationen und ihren Aussagegehalt nicht beeinträchtigen, stellen keine Veränderung der Information dar; Erwägung 43 der ECRL; EBRV 817 BlgNR 21. GP Erläut 3 zu § 13.

[99]) EBRV 817 BlgNR 21. GP Erläut 3 zu § 13.

mittlung gem § 13 Abs 2 ECG). Der Provider haftet nicht, wenn er die Informationen **nicht verändert** (Z 1)[100]), die Bedingungen für den Zugang zur Information beachtet (Z 2)[101]), die Regeln für die Aktualisierung der Information, die in allgemein anerkannten Industriestandards festgelegt sind, beachtet (Z 3)[102]), die zulässige Anwendung von Technologien zur Sammlung von Daten über die Nutzung der Information, die in allgemein anerkannten und verwendeten Industriestandards festgelegt sind, nicht beeinträchtigt (Z 4)[103]) und **unverzüglich eine von ihm gespeicherte Information entfernt, sobald er tatsächlich davon Kenntnis erhalten** hat, dass die Information am ursprünglichen Ausgangsort der Übertragung aus dem Netz entfernt oder der Zugang zu ihr gesperrt wurde oder dass ein Gericht oder eine Verwaltungsbehörde die Entfernung oder Sperre angeordnet hat (Z 5)[104]). Im letzten Fall der Z 5 (Anordnung einer Sperre) ist eine Entfernung des illegalen Inhalts im Proxy-Cache des Diensteanbieters/Providers aber sinnlos, soweit nicht auch der originäre Inhalt tatsächlich entfernt/gelöscht wird: Durch jede neuerliche Anfrage eines Nutzers erfolgt eine neuerliche (automatische) Zwischenspeicherung im Cache des Diensteanbieters. Eine Entfernung der Inhalte aus dem Proxy-Cache ist technisch nicht möglich, soweit die originären Inhalte nicht auch tatsächlich gelöscht/gesperrt sind. Die Erläut stellen deshalb klar, dass Z 5 auch voraussetzt, dass der verantwortliche Host die entsprechenden Maßnahmen bereits veranlasst hat[105]). Zum Begriff der „tatsächlichen Kenntnis" s unter 4.

4. Haftungsbefreiung beim Speichern (§ 16 ECG, Art 14 ECRL)

§ 16 Abs 1 ECG regelt die Verantwortung der Diensteanbieter für die Speicherung fremder Inhalte *(Hosting)*: Demnach besteht **keine Verantwortung,** wenn der Provider (beim Speichern) **von einer rechtswidrigen Tätigkeit oder Information keine tatsächliche Kenntnis** hat (Z 1), **oder** er, sobald er diese Kenntnis erlangt hat, **unverzüglich,** also ohne schuldhaftes Zögern[106]), **tätig wird, um die Information oder den Zugang zu ihr zu sperren** (Z 2). Stammt der rechtswidrige Inhalt von einem dritten Nutzer (also zB dem Schreiber eines Leserbriefs), mit dem der Provider in keiner vertraglichen Verbindung steht, muss der Provider den Diensteanbieter, mit dem er in Vertragsbeziehung steht, also zB den Betreiber eines Forums, veranlassen, die Information herauszunehmen[107]). Als fremde **Inhalte** können Websites, aber auch nur Beiträge (zB Leserbriefe) gespeichert werden[108]).

„Tatsächliche Kenntnis" entspricht nach der RV „in etwa" der **Wissentlichkeit** iSd § 5 Abs 3 StGB; so muss der Täter die rechtswidrigen Umstände nicht nur für wahrscheinlich, sondern für gewiss halten[109]). Die Kenntnis muss sich sowohl auf die Information (Tätigkeit) als auch auf die **Rechtswidrigkeit** beziehen, wobei hinsichtlich der Rechtswidrigkeit eine laienhafte Vorstellung genügt[110]). Die „tatsächliche Kenntnis" kann dem Diensteanbieter durch Dritte oder eine Behörde verschafft werden. Das Abstellen auf die Wissentlichkeit ist (va gegenüber dem Urheber) eine **Besserstellung,** weil für die Strafbarkeit (des Urhebers) idR bedingter Vorsatz genügt (§ 7 Abs 1 StGB; für das Verwaltungsstrafrecht genügt gem § 5 Abs 1 VStG sogar Fahrlässigkeit). Es ist nicht ersichtlich, warum diese Begünstigung rechtspolitisch erforderlich war. In der Praxis wird die Wissentlichkeit kaum je nachweisbar sein. Der Provider ist auch **nicht verpflichtet, Hinweisen** Dritter bezüglich rechtswidriger Inhalte auf seinem Server **nachzugehen.**[111])

Neben der Informationspflicht gegenüber Gerichten (§ 18 Abs 2 ECG – s dazu schon oben unter III.B.1. besteht (nur für Host-Provider) auch eine **Informationspflicht gegenüber Verwaltungsbehörden:** Gem § 18 Abs 3 ECG haben die Host-Provider auf Grund der Anordnung einer Verwaltungsbehörde dieser den **Namen und die Adresse der Nutzer** ihres Dienstes, mit denen sie Vereinbarung über die Speicherung von Informationen abgeschlossen haben, zu übermitteln, sofern die Kenntnis dieser Informationen eine wesentliche Voraussetzung der der Behörde übertragenen Aufgaben bildet. § 18 Abs 3 ECG reicht als Rechtsgrundlage nicht aus, soweit es sich um Eingriffe in das Fernmeldegeheimnis handelt; hier sind die entsprechenden Bestimmungen der StPO und des TKG einzuhalten (s unter III.B.1.).

Diensteanbieter haben den Namen und Adresse eines Nutzers ihres Dienstes, mit dem sie Vereinbarungen über die Speicherung von Informationen abgeschlossen haben, auch **auf Verlangen dritten Personen zu übermitteln,** sofern diese ein überwiegendes **rechtliches Interesse** an der Feststellung der Identität des Nutzers und eines bestimmten rechtswidrigen Sachverhalts sowie überdies glaubhaft machen, dass die Kenntnis dieser Information eine wesentliche Voraussetzung für die Rechtsverfolgung bildet (§ 18 Abs 4 ECG). Als Dritte werden hier va Opfer oder Geschädigte in Betracht kommen. Gerichte oder Behörden kommen nicht in Betracht, weil für diese die Sonderregeln des § 18 Abs 2 und 3 ECG gelten bzw deren Auskunftsersuchen sich auf eine gesetzliche Grundlage stützen muss. § 18 Abs 4 ECG steht insofern im Gegensatz zur ECRL als dort nur Gerichten oder Behörden, nicht aber Dritten Zugang zu Nutzerinformationen gewährt wird. Wann ein „überwiegendes rechtliches Interesse" vorliegt, kann nach der RV „in der Praxis Schwierigkeiten bereiten", weshalb diesbezüglich auf die Fähigkeiten eines juristischen Laien abzustellen sei. Nur wenn es auch für den Nichtfachmann **offenkundig** sei, dass eine bestimmte Information gegen die Rechte Dritter verstoße, müssen die Daten herausgegeben werden[112]).

---

[100]) Eingriffe rein technischer Art sind keine Veränderungen (EBRV 817 BlgNR 21. GP Erläut 2 zu § 15; Erwägung 42 ECRL).

[101]) Eine Zugangskontrolle der „gecachten" Internetseite muss weiterhin möglich sein (EBRV 817 BlgNR 21. GP Erläut 2 zu § 15).

[102]) Die „gecachte" Version muss, soweit dies technisch möglich ist, gleich aktuell wie die Originalseite sein (EBRV 817 BlgNR 21. GP Erläut 2 zu § 15).

[103]) So darf der Provider zB Besucherzähler des Seitenbetreibers nicht beeinträchtigen (EBRV 817 BlgNR 21. GP Erläut 2 zu § 15).

[104]) Damit soll verhindert werden, dass im Fall einer (behördlichen) Löschung einer Seite eine „gecachte" Kopie weiterexistiert (EBRV 817 BlgNR 21. GP Erläut 2 zu § 15).

[105]) EBRV 817 BlgNR 21. GP Erläut 2 zu § 15.

[106]) EBRV 817 BlgNR 21. GP Erläut 2 zu § 16.

[107]) EBRV 817 BlgNR 21. GP Erläut 2 zu § 16. Diese „Mutation des Host-Providers vom Vertragspartner zum Richter" bzw die Verpflichtung des Host-Providers zur Zensur wird von *Kilches* (E-Commerce-Gesetz – gelungene Richtlinienumsetzung? MR 2001, 252) im Hinblick auf Art 10 Abs 2 MRK (Freiheit der Meinungsäußerung) zu Recht als verfassungsrechtlich bedenklich eingestuft.

[108]) EBRV 817 BlgNR 21. GP Erläut 1 zu § 16.

[109]) EBRV 817 BlgNR 21. GP Erläut 3 zu § 16.

[110]) EBRV 817 BlgNR 21. GP Erläut 3 zu § 18; *Brenn,* Der elektronische Geschäftsverkehr, ÖJZ 1999, 488.

[111]) EBRV 817 BlgNR 21. GP Erläut 3 zu § 16.

[112]) EBRV 817 BlgNR 21. GP Erläut 3 zu § 18.

C. Haftung nach dem TKG[113])

§ 75 Abs 1 TGK (früher: § 16 FernmeldeG) bestimmt, dass **Funkanlagen** und **Endgeräte nicht missbräuchlich verwendet werden dürfen.** Die technischen Einrichtungen des Providers (insb Webserver) sind in diesem Zusammenhang als Endgeräte iSd § 3 Z 2 TKG, er selbst als Betreiber eines Endgeräts zu qualifiziern[114]). Als missbräuchliche Verwendung gilt ua jede **Nachrichtenübermittlung,** welche die öffentliche Ordnung und Sicherheit oder die Sittlichkeit gefährdet oder welche **gegen die Gesetze** verstößt (§ 75 Abs 1 Z 1 TGK). Gegen die Gesetze verstoßen zB Nachrichten mit Inhalten, die gegen das StGB, das VG oder das PornG verstoßen[115]). Nach § 75 Abs 1 **Z 2** TKG gilt als missbräuchliche Verwendung ferner jede grobe Belästigung oder Verängstigung anderer Benützer. Unter Belästigung fallen etwa die Beschimpfung oder Verhöhnung anderer Benutzer; Verängstigung ist gegeben, wenn jemand in Furcht und Unruhe versetzt wird, insb, wenn sich bei den Betroffenen echte Besorgnis für die Zukunft einstellt[116]).

Inhaber von Endgeräten[114]) haben, soweit ihnen dies zumutbar ist, **geeignete Maßnahmen** zu treffen, **um eine missbräuchliche Verwendung auszuschließen.** Diensteanbieter, die lediglich den Zugang zu Telekommunikationsdiensten vermitteln, gelten ausdrücklich nicht als Inhaber **(§ 75 Abs 2 TKG)** – demgemäß fallen die bloßen Access-Provider nicht unter diese Verpflichtung[117]). Nach dem ECG, das ja auch die verwaltungsstrafrechtliche Verantwortlichkeit der Diensteanbieter regelt (s III.B.1.), sind die Diensteanbieter der §§ 13 bis 17 ECG, also insb die Host-Provider aber nicht dazu verpflichtet, die von ihnen gespeicherten oder übermittelten Informationen allgemein zu überwachen oder von sich aus nach Umständen zu forschen, die auf eine rechtswidrige Tätigkeit hinweisen (§ 18 Abs 1 ECG). Auch besteht für sie keine Verpflichtung, qualifizierten Hinweisen nachzugehen (s III.B.1.). Damit bestehen auch für die Host-Provider hinsichtlich § 75 Abs 2 TKG wohl keine Verpflichtungen mehr.

Gem **§ 104 Abs 1 TKG** begeht eine **Verwaltungsübertretung** und ist mit einer Geldstrafe **bis zu 3.633 EUR** zu bestrafen, wer entgegen § 75 Abs 1 ein Endgerät missbräuchlich verwendet (Z 5) oder entgegen § 75 Abs 2 nicht geeignete Maßnahmen trifft, die eine missbräuchliche Verwendung von Funkanlagen oder Endgeräten ausschließen (Z 6). Hier kommt insb eine Begehung durch Unterlassen in Betracht, wenn der Provider dieser Verpflichtung nicht nachkommt. Nach der **Subsidiaritätsklausel** des § 104 Abs 4 TKG entfällt aber die Strafbarkeit gem Abs 1, wenn die Tat den Tatbestand einer in die Zuständigkeit der Gerichte fallenden strafbaren Handlung bildet oder nach anderen Verwaltungsstrafbestimmungen mit strengerer Strafe bedroht ist. Gegenstände, mit denen die Straftat begangen wurde (zB Server, PCs, Modems), können gem § 104 Abs 5 TKG im Straferkenntnis zu Gunsten des Bundes für verfallen erklärt werden.

IV. Haftung des Linksetzers

A. Allgemeines

Für den Linksetzer kommt eine Haftung als unmittelbarer Täter nicht in Frage. Setzt er selbst eine wortlautkonforme Ausführungshandlung, indem er sich mit dem Inhalt der verlinkten Seite identifiziert (insb durch Gutheißen der verlinkten Inhalte) oder sich deren Inhalte sonst zu Eigen macht (zB durch Verwendung fremder Inhalte in eigenen *Frames*[118])), ist er als Urheber zu betrachten (vgl auch § 17 Abs 2 ECG). Somit kommt für die Haftung eines Linksetzers idR **Beitragstäterschaft** (§ 12 dritter Fall StGB, § 7 VStG) in Betracht: Durch das Setzen des Links fördert der Linksetzer die Tat des Urhebers**,** weil er auf dessen kriminelle Inhalte hinweist[119]). Er fördert die Tat auch dann, wenn er ein Link in fremdem Namen setzt oder seine Seite in fremdem Namen betreibt[120]). Enthält der Link selbst rechtswidrige Inhalte (zB ein Hakenkreuz-Bild), ist der Linksetzer diesbezüglich wie ein Urheber zu behandeln. Gleiches gilt, wenn eigene Inhalte (durch interne Links) verlinkt werden.

Die Verweisung via Link kann ein strafbares **Tun oder Unterlassen** (§ 2 StGB) darstellen. Ersteres liegt dann vor, wenn der Linksetzer zum Zeitpunkt, da er den Link setzt, bereits auf eine Seite mit kriminellen Inhalt verweist; Strafbarkeit durch Unterlassen kommt in Betracht, wenn der kriminelle Inhalt vom Urheber erst nach der Linksetzung in der verlinkten Seite aufgenommen wurde und der Linksetzer den Link trotzdem weiter bestehen lässt. Hier gelten die zu den Providern getroffenen Überlegungen (III.A.) sinngemäß.

Auf der inneren Tatseite ist (wie beim Host-Provider) erforderlich, dass der Linksetzer tatsächliche **Kenntnis der rechtswidrigen Information** (§ 17 Abs 1 ECG) oder Tätigkeit auf der verlinkten Seite hat. IdR wird davon auszugehen sein, dass der Setzer eines Links Kenntnis vom Inhalt der Seite hat, auf die er verweist: Wer entsprechende Verweise einrichtet, sieht sich gewöhnlich auch die verknüpften Inhalte an. Das gilt aber nur für den Inhalt zum Zeitpunkt der Linksetzung, da sich die Inhalte im Internet durch Aktualisierung sehr schnell ändern können[121]). Da der Linkset-

---

[113]) Telekommunikationsgesetz, BGBl I 1997/100. Siehe dazu *Holoubek/Lehofer/Damjanovic,* Grundzüge des Telekommunikationsrechts, 2000; *Schmölzer/Mayer-Schönberger,* Das Telekommunikationsgesetz 1997, ÖJZ 1998, 378; *Zanger/Schöll,* Telekommunikationsgesetz. Kommentar (2000).

[114]) Zum Begriff des „Endgeräts" s FN 75. Anzumerken ist, dass neben dem *Provider* auch der *Urheber* von Inhalten als Inhaber eines Endgeräts iSd § 3 Z 2 TKG anzusehen ist; handelt es sich um gesetzeswidrige Inhalte, so kommt auch für ihn eine Haftung nach dem TKG (als unmittelbarer Täter wegen missbräuchlicher Verwendung eines Endgeräts) in Betracht (*Schmölzer* in StPG 25, 153 mwN). Als „Inhaber von Endgeräten" gelten aber (unverständlicherweise) nicht nur die „Sender" von Nachrichten, sondern auch die Empfänger, also jeder *Konsument* (s dazu unter VI.). Und schließlich fallen auch die Linksetzer unter § 75 TKG, da auch sie Endgeräte benützen.

[115]) *Zanger/Schöll,* TKG § 75 Rz 5.

[116]) *Zanger/Schöll,* TKG § 75 Rz 10 f.

[117]) RV 759 BlgNR 20. GP 56; somit trifft den reinen Access-Provider nach dieser Bestimmung auch bei Kenntnis von rechtswidrigen Daten auf seinem Server keine Verpflichtung einen Missbrauch zu verhindern. Allerdings wird diese Haftungsbefreiung kaum zur Anwendung kommen, weil „reine" Access-Provider in Österreich kaum existieren (s oben I.B.).

[118]) Ein Frame teilt die Anzeigefläche eines Browsers in voneinander unabhängige Bereiche auf, von denen jeder eine eigene HTML-Datei anzeigt, die auch unabhängig voneinander verändert, zB gescrollt, werden kann.

[119]) AA *Brenn,* ÖJZ 1999, 489.

[120]) Zur Linksetzung in fremden Namen vgl zB den Sachverhalt der (zivilrechtlichen) OGH-E 12. 9. 2001, 4 Ob 176/01 p = EvBl 2002/22 („fpo.at"): Der in Amerika lebende Alain L. hatte unter der bei der Beklagten nic.at registrierten Domain fpo.at eine Website erstellt, die im Wesentlichen mit der Homepage der klagenden Partei FPÖ identisch war. Allerdings wurde sie mit Links zu Neonazi-Seiten und dem Horst-Wessel-Lied versehen.

[121]) Vgl AG Berlin-Tiergarten 30. 6. 1997, 260 DS 857/96, MMR 1998, 49 f mit Anm *Hütig* = CR 1998, 111 mit Anm *Vassilaki.*

zer als Beitragstäter haftet, muss außerdem der (zumindest bedingte) Vorsatz auf die Förderung der Haupttat vorliegen. Die Tat ist gerechtfertigt, wenn der Linksetzer rechtswidrige Inhalte verlinkt, die er eben wegen dieser Rechtswidrigkeit kritisiert[122]). Hier will der Linksetzer ja gerade verhindern, dass die Inhalte in Zukunft weiterverbreitet werden bzw aufklären und dazu anregen, solche Inhalte zu entfernen.

Hinsichtlich **„Haftungssauschließungsklauseln",** die der Linksetzer erklärt (zB durch den Vermerk: „Für den Inhalt der angegeben Adressen wird keine Haftung übernommen") ist jeweils im Einzelfall zu prüfen, ob damit wirklich eine Distanzierung von den kriminellen Inhalten erfolgen sollte, oder ob eine bloße „Alibihandlung" vorliegt, der Linksetzer in Wirklichkeit die Haupttat trotzdem fördern wollte (wenn sich zB auf der Seite des Linksetzers ergibt, dass er zu den Inhalten, auf die er verweist, eine positive Einstellung hat).

Wie für den Urheber und Provider kommt auch für den Linksetzer eine (subsidiäre) verwaltungsstrafrechtliche Haftung gem § 104 Abs 1 iVm § 75 TKG, Art IX Abs 1 Z 4 EGVG und § 3 Abs 1 iVm § 1 Abs 1 AbzeichenG in Betracht.

Der OGH hat sich bislang mit der „Linkhaftung" nur im Wettbewerbsrecht auseinander gesetzt[123]). Diese Rsp kann aber auf das Strafrecht nicht übertragen werden[124]).

B. Haftungsausschluss nach § 17 ECG

Das ECG regelt erstmalig in Österreich die (straf-, verwaltungsstraf- und zivilrechtliche) Haftung für das Setzen von Links, also für Konsumenten nutzbare elektronische Verweise/Verbindungen zu anderen Web-Sites. Das ECG geht mit seiner Regelung dabei über die Vorgaben der ECRL hinaus, welche die Linkhaftung nicht regelt. Wie schon beim Provider schließt das ECG unter gewissen Voraussetzungen die Haftung des Linksetzers nach dem StGB, VG, PornG, TKG usw aus („Filterwirkung" des ECG). Der Strafausschließungsgrund des § 17 Abs 1 ECG gilt insb auch für **private Linksetzer,** da unter Diensteanbieter iSd des 5. Abschnitts des ECG auch Anbieter fallen, die unentgeltlich Informationen im Netz anbieten (s III.B.1.).

§ 17 ECG bestimmt (in Anlehnung an die Haftung der Host-Provider), dass ein Diensteanbieter für die Inhalte der Seiten, auf die verwiesen wird, nicht verantwortlich ist, sofern er (beim Linksetzen) **von einer rechtswidrigen Tätigkeit oder Information keine tatsächliche Kenntnis** hat (Z 1) oder **sobald er diese Kenntnis erlangt hat, unverzüglich tätig wird, um den elektronischen Verweis zu entfernen** (Z 2). Zur Auslegung der Begriffe „tatsächliche Kenntnis**"** s bereits oben unter III.B.4. Wer also zB auf seiner Homepage **wissentlich** Links zu Seiten mit Inhalten setzt, die gegen das VG verstoßen, macht sich wie der Urheber strafbar nach diesem Gesetz[125]). Wie auch die anderen Diensteanbieter trifft aber den Linksetzer keine Verpflichtung, die (via Link) zugänglich gemachten Informationen allgemein zu überwachen oder von sich aus nach Umständen zu forschen, die auf rechtswidrige Tätigkeiten hinweisen (§ 18 Abs 1 ECG).

Problematisch ist die Haftung für **mittelbar verlinkte Inhalte:** Da das ganze Internet mehr oder weniger durch Links vernetzt ist, wäre nach der *conditio-sine-qua-non*-Formel jeder Linksetzer auf Grund der „Linkverkettung" mittelbar für nahezu alle Internet-Inhalte verantwortlich. Die Haftungsfrage ist daher prinzipiell auf jene Seiten zu beschränken, auf die unmittelbar verwiesen wird (direktes Link). **Bei entsprechender Kenntnis** ist nach den Erläut aber auch eine Haftung des Linksetzers für mittelbar verlinkte Inhalte denkbar[126]). So zB, wenn jemand die (keine kriminellen Inhalte enthaltene) Startseite eines Nazi-Seite verlinkt, dies aber mit dem Wissen, dass sich auf einer untergeordneten (durch interne Links mit der Startseite verbundenen) Seite neonazistische Inhalte befinden.

Der Haftungssauschluss des § 17 Abs 1 ECG betrifft nur **elektronische Verweise,** also Links im Internet; werden Internetadressen, die zu kriminellen Inhalten führen, anderswo (zB in Broschüren) publiziert, greift der Haftungsausschluss des ECG nicht.

V. Haftung des Betreibers von Suchmaschinen (§ 14 ECG)

§ 14 ECG legt für den Betreiber einer Suchmaschine (oder andere ähnliche elektronische Hilfsmittel zur Suche nach fremder Information) dieselben Haftungsausschließungsgründe wie für den Access-Provider (§ 16 Abs 1 ECG) fest. Damit geht das ECG über die ECRL hinaus, welche die Haftung solcher Betreiber nicht regelt.

Suchmaschinen oä Hilfsmittel sind alle Online-Dienste (Programme), die eine elektronische Suche nach bestimmten Informationen erleichtern. Somit fallen darunter nicht nur große Suchdienste wie zB „*Yahoo*" oder „*Google*", sondern jedes Suchprogramm bzw jede Datenbank mit Suchfunktion auf einer Website, soweit dort (auch) nach **fremden** (also nicht bloß vom Betreiber der Suchmaschine stammenden) **Inhalten** gesucht werden kann. Wird eine interne Suchmaschine betrieben, haftet der Betreiber für dort angebotenen (eigenen) kriminelle Inhalte als Urheber.

Keine Haftung für den Betreiber von Suchdiensten besteht, wenn er die **Übermittlung** der abgefragten Information **nicht veranlasst** (Z 1), den Empfänger der abgefragten Information **nicht auswählt** (Z 2) **und** die abgefragte **Information weder auswählt noch verändert** (Z 3). Der Betreiber darf mit der abgefragten bzw übermittelten Information also in keiner Weise in Verbindung stehen. Wird zB ein Suchdienst auf das Auffinden krimineller Inhalte ausgerichtet (der Täter betreibt zB einen Suchdienst speziell für neonazistische Inhalte) wird die Information iSd Z 2 ausgewählt[127]). Die „tatsächliche Kenntnis", wie sie beim Linksetzer und Host-Provider vorgesehen ist, ist beim Suchmaschinenbetreiber dagegen irrelevant: Selbst wenn er weiß, dass mit Hilfe seines Suchdienstes (auch) bestimmte kriminelle Inhalte vermittelt werden, ist sein Haftungsprivileg deswegen noch nicht ausgeschlossen.

---

[122]) Vgl zB das Nizkor-Projekt, das Entgegnungen auf die Argumente von Neonazis verfasst und dabei auch Links zu Neonazi-Seiten unterhält (www.nizkor.org/features/qar/refusalt.html).

[123]) OGH 19. 12. 2000, 4 Ob 274y und 4 Ob 225/00t.

[124]) *Zankl,* Haftung für Hyperlinks im Internet, ecolex 2001, 354 (355).

[125]) So auch LGSt Wien 22. 5. 2001, 12f Hv 1528/01. Der Verurteilte hatte auf seiner Homepage Folgendes angekündigt: „Hallo Kameraden! Für Euch habe ich ein paar gute Adressen, die ihr unter den Links findet.". Dort fanden sich dann auch Links zu Internet-Seiten mit nationalsozialistischem Gedankengut wie dem „Thule-Netz" oder der „Stormfront".

[126]) EBRV 817 BlgNR 21. GP Erläut 3 zu § 17 ECG.

[127]) EBRV 817 BlgNR 21. GP Erläut 2 zu § 14 ECG.

VI. Haftung des Konsumenten krimineller Inhalte

Das bloße Lesen, Abspeichern etc von nationalsozialistischen oder rechtsextremen Inhalten im Internet ist **nicht strafbar.** Das mag selbstverständlich erscheinen, ist es aber nicht: Wer etwa kinderpornografische Inhalte vorsätzlich abgespeichert, macht sich strafbar wegen Sich-Verschaffens von pornographischen Darstellungen mit Unmündigen (§ 207 a Abs 3 StGB[128])). Das bloße Ansehen (Konsum) von Kinderpornos ist aber nicht pönalisiert.

Darüber hinaus könnte man noch eine Haftung des Konsumenten nach **§ 286 StGB** (Unterlassung der Verhinderung einer mit Strafe bedrohten Handlung) in Erwägung ziehen: Muss ein Leser krimineller Inhalte diesbezüglich Anzeige (an den Provider oder die Polizei) erstatten, um einer möglichen Bestrafung nach § 286 StGB zu entgehen? Zunächst ist festzuhalten, dass die Äußerungs- und Verbreitungsdelikte prinzipiell als **Dauerdelikte** angesehen werden können, da die abstrakte oder potenzielle Gefahr[129]) die durch sie pönalisiert wird, so lange andauert, so lange die kriminellen Inhalte zugänglich sind. Mit der Einspeisung ins Netz tritt die Vollendung ein; beendet ist das Delikt aber erst, wenn der kriminelle Inhalt wieder aus dem Netz entfernt ist[130]). Die Verhinderungspflicht des § 286 StGB besteht bei Dauerdelikten nach hM[131]) bis zum Zeitpunkt der *Beendigung* der mit Strafe bedrohten Handlung. Allerdings ist nach *Durl*[132]) § 286 StGB richtigerweise durch teleologische Reduktion **auf abstrakte Gefährdungsdelikte nicht anzuwenden,** da im Falle einer mangelnden (konkreten) Gefahr gerade auch der korrumpierende Eindruck (zumindest) des nichthindernden Unterlassens auf die Rechtsgemeinschaft entfällt. Gleiches muss mE entgegen *Durl*[133]) auch für potenzielle Gefährdungsdelikte gelten, da auch diese nicht auf eine konkrete Gefahr abstellen. Der Leser von durch Äußerungs- und Verbreitungsdelikten zugänglich gemachten Inhalten haftet somit nicht nach § 286 StGB, wenn er solche Taten nicht anzeigt.

Überlegen könnte man auch eine **Verwaltungsstrafe gem § 7 zweiter Fall VStG, § 104 Abs 1 Z 5 iVm § 75 Abs 1 TKG,** da der Konsument auch als Inhaber von Endgeräten[75] gem § 3 Z 2 TKG gilt[134]). Man könnte nach dem Wortlaut der Bestimmung die Meinung vertreten, dass der Konsument durch das Aufrufen einer Seite mit kriminellen Inhalten sein Endgerät missbräuchlich gem § 75 Abs 1 Z 1 TKG verwendet, weil er an einer gesetzeswidrigen Nachrichtenübermittlung mitwirkt (bzw diese durch sein Abrufen ermöglicht). ME ist aber dieser Tatbestand durch teleologische Reduktion einschränkend auszulegen: Zwar wirkt der Konsument durch das Abrufen des Inhalts an der Übermittlung mit bzw löst diese aus; das bloße Konsumieren krimineller Inhalte im Internet kann aber nicht strafwürdiger sein als der Konsum krimineller Inhalte außerhalb des Internets (zB in Büchern, Magazinen oder auf Fotos, Videos), welches in Österreich nicht pönalisiert ist. „Nachrichtenübermittlung" ist also einschränkend iS einer *aktiven* Nachrichtenübermittlung, also eines Nachrichten*sendens* auszulegen; Beihilfe (§ 7 VStG) ist nur durch Mitwirken auf der Seite des Senders, also des Urhebers oder Providers, **nicht** aber **durch bloßes Konsumieren eines Inhalts** möglich[135]). Die gegenteilige Auffassung würde zu sachlich nicht gerechtfertigten Ergebnissen führen: So müsste zB derjenige, der sich Kinderpornos im Internet (bloß) ansieht mit Geldstrafe bis zu 3.633 EUR (§ 104 Abs 1 TKG) rechnen, während derjenige, der sich ein Kinderporno-Video (bloß) ansieht, straffrei ist.

VII. Internationales Strafrecht

A. Inlandstaten

Eine Bestrafung des Urhebers, Providers etc in Österreich hängt immer davon ab, ob sich ein **Anknüpfungspunkt für die inländische Gerichtsbarkeit** ergibt: § 62 StGB erklärt das österr Strafrecht auf all jene Taten für anwendbar, die im Inland begangen worden sind **(Territorialitätsprinzip),** gleichgültig ob der Täter In- oder Ausländer ist. Ob eine Tat **im Inland begangen** wurde, ergibt sich aus § 67 Abs 2 StGB: Demnach hat der Täter eine mit Strafe bedrohte Handlung an jedem Ort begangen, an dem er **gehandelt** hat oder hätte handeln sollen (betrifft Unterlassungsdelikte) oder ein dem Tatbild entsprechender Erfolg, also eine von der Tatausführung räumlich und zeitlich abtrennbare Außenwirkung[136]), ganz oder teilweise eingetreten ist oder nach der Vorstellung des Täters hätte eintreten sollen (betrifft den Versuch). Österr Strafrecht gilt daher für all jene Urheber, Provider etc, die im Inland (iS einer körperlichen Anwesenheit) gehandelt haben oder handeln hätten sollen (**Handlungstheorie;** § 67 Abs 2 erster Fall). Wer also zB **von Österreich aus neonazistische Inhalte ins Internet einspeist** oder von Österreich aus auf kriminelle Inhalte via Links verweist, für den ist österr Strafrecht und damit insb das VG etc anwendbar. Auch wer sich vom Ausland aus an einer Inlandstat beteiligt (§ 12 StGB), unterliegt der österr Jurisdiktion (§ 64 Abs 1 Z 8 StGB[137])). So kann zB ein im Ausland ansässiger Provider als Beitragstäter haften, wenn ihm ein Österreicher vom Inland aus mittels *File-Transfer*[138]) neonazistisches Material für eine Website zusendet.

Handeln Urheber, Provider oder Linksetzer im Ausland, könnte man auch die Anwendung von § 67 Abs 2 dritter

---

[128]) Jemand verschafft sich (§ 207 a Abs 3 1. Fall StGB) eine kinderpornographische Darstellung, wenn er sie durch eigenes Zutun (*Bertel/Schwaighofer,* BT II[4] § 207 a Rz 4) in seinen Gewahrsam bringt, zB vom Internet gezielt auf Festplatte oder Diskette speichert; er besitzt (§ 207 a Abs 3 2. Fall StGB) sie, wenn er sie in seinem Gewahrsam hat (ÖJZ-LSK 1999/147).

[129]) Zur Einordnung der Äußerungs- und Verbreitungsdelikte als abstrakte Gefährdungsdelikte s näher unten VII.A.

[130]) Würde man die Äußerungs- und Verbreitungsdelikte als Zustandsdelikte qualifizieren (Vollendung und Beendigung ab dem Zeitpunkt der Veröffentlichung/Verbreitung), wäre eine Beteiligung daran (insb des Providers oder Linksetzers) ab diesem Zeitpunkt nicht mehr möglich.

[131]) ZB *Hinterhofer,* Zum Anwendungsbereich des § 286 StGB, ÖJZ 1995, 495 (496).

[132]) Die Pflicht zur Verhinderung von mit Strafe bedrohten Handlungen gemäß § 286 StGB (1999) 122 ff.

[133]) Die Pflicht zur Verhinderung von mit Strafe bedrohten Handlungen gemäß § 286 StGB 123.

[134]) *Schmölzer/Mayer-Schönberger,* ÖJZ 1998, 382.

[135]) Vgl auch *Zanger/Schöll,* TKG § 75 Rz 2: „Abs 1 verbietet die missbräuchliche Verwendung durch den unmittelbaren Täter"; und § 75 Rz 68: „Der bloße (. . .) Konsum ist noch nicht strafbar".

[136]) *Kienapfel/Höpfel,* AT[9] Z 9 Rz 6.

[137]) *Schwaighofer* in *Triffterer,* StGB-Komm § 62 Rz 18 mwN und § 64 Rz 20.

[138]) Bei dieser Art der Datenübertragung kann der Urheber mit einem entsprechenden Programm via Internet Daten auf seinen Speicherplatz am Webserver des Providers übertragen und damit seine Homepage erstellen oder ändern. IdR bedarf es dafür (sobald der Zugang vom Provider freigeben wurde) keiner weiteren Handlungen des Providers für die Publikation der (neuen/geänderten) Daten.

Fall StGB **(Erfolgstheorie)** überlegen: Gleichgültig von welchem Rechner auf der Welt die Inhalte (Links) eingespeist werden, könnte als Tatort Österreich angesehen werden, wenn der Inhalt (Link) im Inland abrufbar ist und somit der Erfolg im Inland eintritt[139]). Die österr Strafverfolgungsbehörden müssten dann aber auf Grund des Legalitätsprinzips (§ 34 Abs 1 StPO) gegen alle Urheber, Provider oder Linksetzer rechtswidriger Inhalte vorgehen, die im Internet abrufbar sind (das gesamte öffentlich zugängliche Internet „liegt" ja auf Grund der permanenten Abrufmöglichkeit zur Gänze auch im Inland). Das kann aber nicht iSd Gesetzgebers sein und ist auf Grund der ständig wachsenden Zahl von Seiten mit kriminellen Inhalten (s I.A.) auch nicht durchführbar – die Erfolgstheorie ist daher **einschränkend auszulegen**[140]):

Zunächst kommt die Erfolgstheorie nur bei Erfolgsdelikten zur Anwendung; schlichte **Tätigkeitsdelikte** dagegen beinhalten keinen Erfolg und begründen daher eine inländische Strafbarkeit nur, wenn der Täter im Inland gehandelt hat oder hätte handeln sollen. Fraglich ist, ob Äußerungs- und Verbreitungsdelikte einen Erfolg aufweisen oder nicht. ME haben sie, da sie in aller Regel bloß als **abstrakte Gefährdungsdelikte**[141]) anzusehen sind, **keinen Taterfolg**[142]), weil man als Erfolg iS einer Außenwirkung wohl nur eine konkrete, nicht aber eine abstrakte Gefahr ansehen kann. Der Gesetzgeber pönalisiert mit den Äußerungs- und Verbreitungsdelikten die abstrakte Gefahr dass der Leser die verbreiteten oder zugänglich gemachten Inhalte (Aufforderungen, Lügen usw) möglicherweise umsetzt, glaubt usw; der Täter schafft nur eine mögliche, keine wirkliche Gefahr für andere Rechtsgüter. Die bloße Möglichkeit der Abrufbarkeit dieser Inhalte (also das Zugänglichmachen oder Verbreiten) ist daher als eine **reine Tätigkeit** anzusehen. Als Anknüpfungspunkt verbleibt immer noch der Handlungsort: Wenn der Täter im Inland gehandelt hat, liegt inländische Gerichtsbarkeit vor. Dies würde auch der tatsächlichen Verfolgbarkeit entsprechen: Täter, die im Inland gehandelt haben, sind für die österreichischen Behörden leichter zu fassen, als zB amerikanische Mitglieder des Kuk-Klux-Klan, die von den USA aus eine Homepage betreiben: auf Grund der umfassenden Meinungsfreiheit wären sie nach amerikanischen Recht nicht einmal strafbar (s I.A.).

Der **BGH** hat in einer jüngeren Entscheidung[143]) Volksverhetzung gemäß § 130 Abs 1 und Abs 3[59] dStGB als **abstrakt-konkretes Gefährdungsdelikt** (in Österreich: potenzielle Gefährdungsdelikte[144])) qualifiziert. § 130 Abs 1 und Abs 3 dStGB verlangen beide die Tatbegehung „in einer Weise, die geeignet ist, den öffentlichen Frieden zu stören" (vergleichbar mit der „Eignung, die öffentliche Ordnung zu gefährden" gem § 283 Abs 1 StGB). Der BGH sieht dieses Tatbestandsmerkmal als Erfolg an. Bei abstrakt-konkreten Gefährdungsdelikten sei ein Erfolg iSd § 9 dStGB[145]) dort eingetreten, wo die konkrete Tat ihre Gefährlichkeit im Hinblick auf das im Tatbestand umschriebene Rechtsgut entfalten könnte; bei der Volksverhetzung sei dies die konkrete Eignung zur Friedensstörung in Deutschland. Liegt eine solche Eignung vor, sei der tatbestandsmäßige Erfolg im Inland und somit auch inländische Gerichtsbarkeit gegeben.[143] ME ist aber auch eine Eignung zu einer Gefahr noch keine konkrete sondern bloß eine abstrakte Gefahr[146]); auch potenzielle Gefährdungsdelikte sind noch keine Erfolgsdelikte.

Eine weitere Einschränkungsmöglichkeit liegt im Vorsatz des Täters: Nach manchen Autoren[147]) soll eine Tat, deren Erfolg im Inland eingetreten ist, nur dann der inländischen Gerichtsbarkeit unterliegen, wenn ein Erfolgseintritt im Inland vom Täter auch gewollt oder gar beabsichtigt (§ 5 Abs 2 StGB) war **(„finale Zielsetzung des Täters").** Dies ist aber abzulehnen, da für die einschlägigen Verbreitungs- und Äußerungsdelikte vom Gesetz her keine Absicht (in Bezug auf den Tatort) vorliegen muss, sondern bedingter Vorsatz genügt. Und eine Abstellung bloß auf den bedingten (Tatort-)Vorsatz würde hinsichtlich einer Einschränkung nichts bringen, da jeder Urheber, Provider weiß, dass eine Internetseite überall auf der Welt wo ein Internetanschluss besteht, abgerufen werden kann, also auch in Österreich. Überdies stellt das internationale Strafrecht (§§ 62 ff StGB) auf objektive und (außer beim Versuch gem § 67 Abs 2 letzter Fall StGB) nicht auf subjektive Anknüpfungspunkte ab.

Sieber[148]), der an eine eigenständige Auslegung des Erfolgsbegriffs anknüpft, nämlich auf den **„Tathandlungserfolg"**, will die inländische Strafbarkeit bei Äußerungs- und Verbreitungsdelikten dahingehend einschränken, dass der Tatort nur dann im Inland liegt, wenn der Täter im Inland (iSd körperlichen Anwesenheit) gehandelt hat oder (vom Ausland aus) die **kriminellen Inhalte gezielt auf einen inländischen Computer/Server übermittelt** („gepushed") hat; nur dann seien sie im Inland zugänglich gemacht bzw der (Tathandlungs-)Erfolg im Inland eingetreten. Irrelevant sei dagegen, von welchem Ort die Information abgerufen („gepulled") werden kann; es komme vielmehr darauf an, von welchem Computer aus der Täter eine Möglichkeit der Kenntnisnahme eröffnet (Differenzierung nach Push- und Pull-Technologie). Ob der Täter strafbare Inhalte gezielt „pushed" oder sie ohne Präferenz für ein bestimmtes Land ins Internet stellt, macht freilich aus der Sicht der Handlungstheorie keinen Unterschied: Da wie dort hat der Täter gerade nicht im Inland, sondern im Ausland gehandelt.

---

[139]) Diese Auffassung vertreten zB *Auer/Loimer,* ÖJZ 1997, 616.

[140]) Für Österreich gibt es hinsichtlich der Einschränkung der Erfolgstheorie in Bezug auf Verbreitungsdelikte noch keine Literatur. Einen Überblick zum diesbezüglichen Meinungsstand in Deutschland bietet zB *Tröndle/Fischer* (Hrsg), StGB[50] § 9 Rz 5 ff.

[141]) Abstrakte Gefährdungsdelikte sind jene Delikte, bei denen schon die bloße gedankliche (= theoretische = abstrakte) Möglichkeit, dass das Tatobjekt beeinträchtigt werden könnte, zur Tatbestandsverwirklichung ausreicht; *Kienapfel/Höpfel,* AT[9] Z 9 Rz 35. Konkrete Gefährdungsdelikte dagegen sind Erfolgsdelikte. Sie verlangen als Erfolg, dass sich das Opfer im Wirkungsbereich der gefährlichen Handlung befindet oder dorthin gerät; vgl *Bertel/Schwaighofer,* BT I[6] § 89 Rz 1.

[142]) *Schwaighofer* in *Triffterer,* StGB-Komm § 62 Rz 17; ebenso *Sieber,* Internationales Strafrecht im Internet, NJW 1999, 2065 (2068): Es sei gerade das Charakteristikum der abstrakten Gefährdungsdelikte, dass diese keinen Erfolgsort aufweisen. Ebenso *Arzt,* Erfolgsdelikt und Tätigkeitsdelikt, SchwZStR 107/1990, 168 (170): „Was die abstrakten Gefährdungsdelikte betrifft, setzen sie keinen Erfolg (auch keinen Gefahrenerfolg!) voraus, weil die in der Tatbestandserfüllung liegende abstrakte Gefahr sich nicht in eine konkrete Gefahr oder Verletzung umzusetzen braucht."; AA *Schwarzenegger,* Der räumliche Geltungsbereich des Strafrechts im Internet, SchwZStR 118/2000 (124f), wonach der Erfolg bei abstrakten Gefährdungsdelikten an allen Orten liegt, in denen sich die Gefahr realisieren könnte.

[143]) BGH 12. 12. 2000, 1 StR 184/00; abgedruckt in CR 2001, 260 mit Anm *Vassilaki.*

[144]) Der Tatbestand potenzieller Gefährdungsdelikte ist dann erfüllt, wenn im Einzelfall die „typische Eignung" eines bestimmten Verhaltens „zur Herbeiführung einer konkreten Gefahr" vom Gericht festgestellt wird; *Nowakowski* in WK Vorbem §§ 3–5 Rz 23.

[145]) Ähnlich wie § 67 Abs 2 StGB bestimmt § 9 dStGB: „Eine Tat ist an jedem Ort begangen, an dem der Täter gehandelt hat oder hätte handeln müssen oder an dem der zum Tatbestand gehörende Erfolg eingetreten ist oder nach den Vorstellungen des Täters eintreten sollte."

[146]) IdS auch *Steininger* in WK[2] (§ 283 Rz 15): „Der Tatbestand lässt die Eignung, die öffentliche Ordnung zu gefährden genügen und erfasst demnach schon deren abstrakt potenzielle (und nicht erst konkrete) Gefährdung."

[147]) ZB *Thiele,* Straftaten im Cyberspace, MMR 1998, 219 (224); *Oehler,* Internationales Strafrecht[2], 1983, 212 ff, Rz 253 ff; *Collardin,* Straftaten im Internet, CR 1995, 618 (620); *Conradi/Schlömer,* Die Strafbarkeit der Internet-Provider, 1. Teil, NStZ 1996, 366 (369).

[148]) NJW 1999, 2071 f.

B. Auslandstaten

Liegt weder der Erfolgs- noch der Handlungsort im Inland, so liegt inländische Gerichtsbarkeit unter den folgenden Voraussetzungen des **§ 65 StGB** vor: Der Täter muss entweder Österreicher sein (Abs 1 Z 1) oder ein Ausländer, der im Inland betreten wurde und aus einem bestimmten Grund nicht ausgeliefert werden kann (Abs 1 Z 2); der Strafanspruch darf jedoch im Ausland noch nicht realisiert worden (Abs 4 Z 3) und die Tat muss **auch nach den Gesetzen des Tatorts strafbar** sein (Abs 1; Prinzip der identen Norm). Letzteres wird für „NS-Wiederbetätigungsdelikte" aber selten der Fall sein, weil, abgesehen von Deutschland (§ 130 Abs 3 dStGB), in anderen Staaten idR keine dem VG entsprechende Regelung existiert.

Manche strafbare Handlungen im Ausland werden im Gegensatz zu § 65 StGB unabhängig davon bestraft, ob sie im Ausland strafbar sind oder nicht (**§ 64 StGB;** Prinzip der Weltstrafrechtspflege): Darunter fallen insb die pornographischen Darstellungen mit Unmündigen gem § 207 a Abs 1 und Abs 2 StGB, sofern der Täter Österreicher ist und seinen gewöhnlichen Aufenthalt im Inland hat (§ 64 Abs 1 Z 4 a StGB). Strafbare Handlungen nach dem VG oder den §§ 281 ff StGB fallen mangels dortiger Auflistung nicht unter § 64 StGB.

C. Herkunftslandprinzip[149])

Nach § 20 ECG gilt **für kommerzielle Diensteanbieter** (und nur für sie: § 3 Z 8, 1, 2 ECG) unter gewissen Voraussetzungen das Recht ihres (EU-)Niederlassungsstaates, va was die „rechtliche Verantwortlichkeit" angeht. Da neonazistische Inhalte in aller Regel unentgeltlich verbreitet werden, spielt das Herkunftslandprinzip für die vorliegende Untersuchung keine Rolle (sehr wohl aber, wenn zB Kinderpornographie gegen Entgelt im Internet angeboten wird).

VIII. Strafverfolgung und Bekämpfung des Neonazismus im Internet

Zur Bekämpfung des Neonazismus im Internet kommen mehrere Gruppen von Akteuren in Betracht: Zunächst die **Konsumenten** indem sie einschlägige Seiten den zuständigen **Behörden** oder **Hotlines** melden oder indem sie (insb Eltern oder Schulen) kriminelle Inhalte herausfiltern; dann die (Host-)**Provider,** ebenfalls durch Anzeigen oder durch freiwillige Selbstkontrolle und/oder Filterung ihrer Angebote; weiters der **Staat** durch die Schaffung der gesetzlichen Rahmenbedingungen; und schließlich **internationale Organisationen** durch entsprechende Übereinkommen.

A. Derzeitige Praxis

Wie die Praxis zeigt, wurden in Österreich bereits mehrere Personen auf Grund der Verbreitung rechtswidriger Inhalte im Internet verurteilt. Der Großteil der Fälle betrifft das Zugänglichmachen sowie den Besitz von Kinderpornographie. Aber auch nach dem VG wurden schon Urteile ausgesprochen[150]). Bei der Exekutive wurde eine eigene Gruppe von **„Cyberpolizisten"** ausgebildet, die das Internet nach kriminellen Inhalten durchforsten, Hinweisen darauf nachgehen und verdächtige Seiten der StA bekannt geben. Die Spezialisten sind Teil der internationalen „Cyber-Crime-Unit" und arbeiten mit Experten der internationalen Polizeibehörden (Interpol) zusammen[151]). Weiters hat das BMI ein „virtuelles Wachzimmer" mit einer Meldestelle für Kinderpornographie eingerichtet. In Anbetracht der ständig steigenden Zahl rechtsextremer Internet-Inhalte wäre es sinnvoll, beim BMI auch eine entsprechende „Meldestelle für Neonazismus" einzurichten. Damit allein kann aber noch nicht das Auslangen gefunden sein: Es bedarf zusätzlich einer ausreichenden Anzahl entsprechend geschulter Beamter und die entsprechende Technik zur Durchforstung des Internets nach kriminellen Inhalten.

Es existieren auch **private Initiativen,** um die ständig wachsende Flut von kriminellen Inhalten im Internet zu bekämpfen: So haben sich die **ISPA** (Internet Service Providers Austria – ein Verein von ca 200 inländischen Providern) **Verhaltensrichtlinien** (ISPA-RL) erstellt, denen sich alle Mitglieder unterwerfen müssen: In § 4 Abs 1 ISPA-RL wird darauf hingewiesen, dass Internet-Inhalte den jeweils anwendbaren österr Gesetzen unterliegen und dass ISPA-Provider nach Kenntnis von öffentlich zugänglichen, strafrechtlich relevanten Inhalten den Zugang zu diesen mit technisch und wirtschaftlich vertretbaren Mitteln unterbinden werden. Außerdem hat die ISPA unter http://hotline.ispa.at eine virtuelle **Meldestelle** eingerichtet; dort werden anonyme Meldungen über Kinderpornographie oder Neonazismus entgegengenommen, geprüft und gegebenenfalls an die (Staats-)polizei sowie an den zuständigen Provider weitergeleitet. Bei ausländischen Verbindungen werden die Behörden ebenfalls kontaktiert, darüber hinaus auch die Partner-Vereinigungen im jeweiligen Land. Die ISPA arbeiten überdies eng mit einem internationalen Netz namens „Inhope" (Internet Hotline Providers in Europa) zusammen. Bei Kenntnis illegaler Inhalte, die sich in ihrem Einflussbereich befinden, haben die ISPA-Mitglieder mittels ihnen zur Verfügung stehender, zumutbarer Handlungen **unverzüglich den Zugang zu diesen Inhalten zu sperren** bzw nachweislich die unverzügliche Sperre des Zugangs zu diesen Inhalten zu veranlassen, falls sich der betroffene Server im Einflussbereich ihrer Kunden befindet (§ 4 letzter Absatz ISPA-RL). Jedes Mitglied verpflichtet sich, den Verhaltenskodex zu unterstützen und umzusetzen (§ 8 Abs 1 ISPA-RL). Bei Zuwiderhandeln stehen dem Vorstand der ISPA je nach Schwere und Häufigkeit der **Nichtbeachtung** der Richtlinien durch das betroffene ISPA-Mitglied die Mittel der Ermahnung des Betroffenen oder die **Beendigung von dessen Mitgliedschaft** zur Verfügung (§ 8 letzter Absatz ISPA-RL).

B. Technische Möglichkeiten

Eine Möglichkeit der Bekämpfung krimineller Internet-Inhalte, die zT schon angewandt wird, ist die Verwendung von **Filterprogrammen** (durch die Provider oder Konsumenten) zur Überwachung des elektronischen Verkehrs: Diese Programme überprüfen die abgerufenen Informationen und filtern kriminelle Inhalte heraus. Doch selbst wenn die Software gut genug ist, um nicht umgangen zu werden, wird da-

[149]) Eingehend dazu *Ebensperger/Venier,* Internet und Strafrecht, in *Brenn* (Hrsg), E-Commerce-Gesetz. Kommentar, 2002 (in Druck).

[150]) Wie zB LGSt Wien 22. 5. 2001, 12 f Hv 1528/01.

[151]) IT-Kriminalität gefährlicher als Organisierte Kriminalität, Der Standard 14. 5. 2001.

durch die Verantwortung von den Staaten auf die Provider bzw Konsumenten verlagert. Außerdem sind die meisten Filterprogramme technisch noch nicht ausgereift: Sie suchen meist nach bestimmten Schlagwörtern (wie zB „Hitler" oder „Kindersex") und filtern dann Seiten mit Inhalten, in denen die gesuchten Wörter vorkommen, heraus **(„Keyword-Blocking").** Allerdings werden damit auch Seiten gesperrt, die sich kritisch, aufklärend, wissenschaftlich oder journalistisch mit solchen Inhalten auseinander setzen. Auch das **„Site-Blocking"** (Sperren bestimmter einschlägiger Seiten) erscheint wenig Erfolg versprechend: Dabei muss der Provider die Internet-Adressen der zu sperrenden Seiten kennen, was auf Grund der ständig wachsenden Zahl dieser Seiten und der Spiegelungsmöglichkeit (vgl I.A.) nur zT möglich ist. Schließlich haben Filter nur eine begrenzte Wirkung: Sie filtern maximal jene Seiten mit kriminellen Inhalten heraus, die der Konsument über jene Provider (die ein Filterprogramm anwenden) abruft. An der weiteren Existenz und sonstigen Abrufmöglichkeit dieser Seiten ändert sich aber nichts.

C. Internationale Rechtsakte

Wichtigster einschlägiger Rechtsakt der **EU** ist die erwähnte **E-Commerce-Richtlinie** (s III.B.) aus dem Jahr 2000. Aber schon 1999 verabschiedete der Rat und das EP einen 4-jährigen „**Aktionsplan** zur Förderung der sicheren Nutzung des Internet durch die Bekämpfung illegaler und schädlicher Inhalte in globalen Netzen".[152]) Ziel des Aktionsplans ist neben der Entwicklung von Filter- und Bewertungssystemen die Schaffung eines europäischen „Hotline-Netzes", welches es den Konsumenten ermöglichen soll, bedenkliche Netz-Inhalte anzuzeigen.

Im November 2001 erging seitens der EU-Kommission ein Entw für einen **Rahmenbeschluss** betreffend **rassistische und fremdenfeindliche Straftaten.**[153]) Zu den im Vorschlag aufgeführten Straftaten zählen ua die öffentliche Aufstachelung zu rassistischer und fremdenfeindlicher Gewalt bzw zu Rassen- und Fremdenhass. Solche Verhaltensweisen sollen mit einer Freiheitsstrafe im Höchstmaß von mindestens zwei Jahren geahndet werden. Auch die öffentliche Verbreitung von rassistischem Material via Internet soll künftig in jedem Mitgliedstaat als Straftat eingestuft werden. Damit soll sichergestellt werden, dass Rassismus und Fremdenfeindlichkeit in allen Mitgliedstaaten mit einheitlichen, wirksamen, angemessenen und abschreckenden Strafen geahndet werden. Selbstverständlich steht es den Mitgliedstaaten frei, weiterreichende Maßnahmen zu treffen.

Art 4 lit a des Internationalen **Übereinkommens** der Vereinten Nationen über die **Beseitigung aller Formen rassischer Diskriminierung** (BGBl 1972/377) verpflichtet die Vertragsstaaten, **jede Verbreitung** von Ideen, die sich auf der Überlegenheit einer Rasse oder den Rassenhass gründen, jedes Aufreizen zur rassischen Diskriminierung sowie alle Gewaltakte oder jegliche Aufreizung dazu gegen irgendeine Rasse oder Gruppe von Personen anderer Hautfarbe oder ethnischen Herkunft sowie jegliche Unterstützung rassistischer Betätigung **unter Strafe zu stellen.** Die Umsetzung in Österreich erfolgte durch § 283 StGB (s II.A.3.).

[152]) Entscheidung Nr. 276/1999/EG Des Europäischen Parlaments und des Rates vom 25. 1. 1999.

[153]) Dzt noch nicht im Amtsblatt.

Im **„Cybercrime-Übereinkommen"**[154]) des Europarats findet sich neben Regelungen zur „klassischen" Computerkriminalität („Hacking" etc) als einzige inhaltsbezogene Straftat die Verbreitung von Kinderpornographie (Art 9); auf Aufrufe zu Gewalt und Rassenhass etc wird nicht eingegangen.

D. Zukünftige gesetzliche Maßnahmen

Zunächst ist festzuhalten, dass effektive gesetzliche Maßnahmen zur Bekämpfung krimineller Inhalte und die Durchsetzung nationaler Strafgesetze im globalen Medium Internet auf Grund der weltweiten Einspeisungsmöglichkeit von Daten nur im internationalen Kontext greifen können. Überlegenswert wäre daher ein **internationales** oder zumindest europäisches[155]) **Abkommen über die Nutzung des Internets.** Damit müssten einheitliche Mindeststandards hinsichtlich krimineller Inhalte sowie eine internationale Instanz geschaffen werden, wo solche Inhalte gemeldet werden können, damit es (schneller) zur Eliminierung einschlägiger Seiten kommt. Sinnvoll wäre auch die Schaffung eines **Zusatzprotokolls zum Cybercrime-Übereinkommen** des Europarats betreffend strafrechtliche Mindeststandards bezüglich Gewalt verherrlichender oder rassistischer Internet-Inhalte. Damit einhergehend wäre eine **verstärkte internationale Kooperation** bei der Bekämpfung und Verfolgung von Anbietern illegaler Inhalte wünschenswert, am besten im Zusammenhang mit einer möglichst weitgehenden Angleichung der materiellen Strafrechtsvorschriften im Hinblick auf die Verbreitung Gewalt verherrlichender, rassistischer uä Inhalte. Daneben sollte die Weiterentwicklung von Filtersoftware gefördert und evtl die Provider verpflichtet werden, anhand einer „Negativ-Liste" bekannte Seiten mit kriminellen Inhalten für die Konsumenten zu sperren („Site-Blocking"). Diese Liste sollte von einer international anerkannten Instanz laufend aktualisiert werden und im Internet zwecks Integration in Filterprogramme frei erhältlich sein.

Abschließend ist darauf hinzuweisen, dass Inhalte im Internet immer auch ein Spiegelbild der Gesellschaft sind. Um das Problem an der Wurzel zu bekämpfen, ist eine verstärkte Aufklärung über Neonazismus, Rassismus und Rechtsextremismus sowie die Herstellung von Gegenöffentlichkeit notwendig. Die Arbeit antirassistischer Initiativen sollte mehr gefördert werden. Vor allem im Internet selbst müssten mehr anti-neonazistische und aufklärende Seiten entstehen. Hier sollte man auch auf staatlicher Seite deutlich mehr unternehmen und finanzielle Mittel freigeben.

IX. Zusammenfassung

Die Zahl der Internetseiten mit neonazistischen, rassistischen und Gewalt verherrlichenden Inhalten hat ein Besorgnis erregendes Ausmaß erreicht und ist ständig im Ansteigen. Grundsätzlich haften die Urheber solcher Inhalte nach den einschlägigen Vorschriften im StGB und im VG. Neben der kriminalstrafrechtlichen Haftung kommt (subsidiär)

[154]) Convention on Cyber-Crime vom 23. 11. 2001, ETS Nr. 185; Österreich hat das Übereinkommen unterzeichnet, aber noch nicht ratifiziert.

[155]) Dass die angloamerikanischen Staaten, allen voran die USA ein solches Abkommen unterzeichnen werden ist auf Grund des umfassenden Rechts auf Meinungsäußerung unrealistisch (s unter I.A.). Aus demselben Grund kann auch keine weit reichende Harmonisierung des materiellen Strafrechts erwartet werden.

auch die Anwendung von Verwaltungsstrafbestimmungen nach dem EGVG, dem AbzeichenG sowie dem TKG in Betracht.

Neben dem Urheber krimineller Inhalte haftet uU auch der Provider, also derjenige, der die Verbreitung der Inhalte im Internet durch Zugangsvermittlung oder Bereitstellen von Speicherplatz *(Hosting)* technisch ermöglicht. Das E-Commerce-Gesetz sieht für bestimmte Provider Strafausschließungsgründe vor: So kommt zB für einen Host-Provider keine Haftung in Betracht, wenn er von der rechtswidrigen Tätigkeit oder Information keine tatsächliche Kenntnis hat oder er, sobald er diese Kenntnis hat, unverzüglich tätig wird, um die entsprechende Seite zu sperren (§ 16 Abs 1 ECG). Provider, die dem Verbreiter lediglich den Zugang zum Internet vermitteln (Access-Provider) haften nicht, sofern sie mit der Information (abgesehen von der Zugangsvermittlung) nicht in irgendeiner Form in Verbindung stehen (vgl § 14 ECG).

Neben dem Verbreiter und dem Provider haftet unter gewissen Voraussetzungen auch der „Linksetzer", also derjenige, der auf rechtswidrige Inhalte via Hyperlink verweist. Die Haftungssauschließungsgründe sind hier ähnlich geregelt wie beim Host-Provider (vgl § 18 ECG). Linksetzer und Provider haften, sofern keine Haftungsausschließungsgründe nach dem ECG vorliegen, nach denselben kriminal- und verwaltungsstrafrechtlichen Bestimmungen wie der Urheber; in aller Regel wird (bei entsprechendem Vorsatz) eine Strafbarkeit als Beitragstäter vorliegen. Auch die Strafbarkeit durch Unterlassen spielt für Provider und Linksetzer eine Rolle, insb dann, wenn sie trotz Kenntnis des kriminellen Inhalts einer Seite diese (gezielt) nicht sperren bzw das darauf verweisende Link nicht sofort entfernen. Im Gegensatz zum Urheber, Provider und Linksetzer haftet der Konsument, der die neonazistischen Inhalte bloß liest oder abspeichert (downloadet), nicht.

Da es sich bei den einschlägigen Straftatbeständen des VG und des StGB idR um schlichte Tätigkeitsdelikte handelt, liegt nach dem Territorialitätsprinzip (§ 62 StGB) und der Handlungstheorie (§ 67 Abs 2 erster Fall StGB) ein Anknüpfungspunkt für die österr Gerichtsbarkeit nur dann vor, wenn der Urheber, Provider oder Linksetzer in Österreich gehandelt hat. Eine Anwendung der Erfolgstheorie (unter der Prämisse, dass die Verbreitung der kriminellen Inhalte im Internet einen Erfolg darstellt) würde zu einer Zuständigkeit der österr Strafgerichtsbarkeit für alle Inhalte im Internet führen, die gegen das Verbotsgesetz, StGB etc verstoßen. Ein – insb im Hinblick auf die praktische Durchführbarkeit – unerwünschtes Ergebnis: Die österr StA wären auf Grund des Legalitätsprinzips zur Verfolgung aller (amtsbekannten) kriminellen Internet-Inhalte verpflichtet. Handelte der Täter vom Ausland aus, besteht eine Zuständigkeit der inländischen Gerichte nur unter den Voraussetzungen des §§ 65 und 64 Abs 1 Z 8 StGB.

Um den Neonazismus im Internet effektiv bekämpfen zu können, bedarf es auf rechtlicher Basis eines verstärkten internationalen Vorgehens. Neben der E-Commerce-Richtlinie der EG (die in Österreich durch das ECG umgesetzt wurde) bestehen derzeit keine effektiven einschlägigen internationalen Regelungen (ein einschlägiger EU-Rahmenbeschluss befindet sich dzt erst im Entwurfsstadium). Eine mögliche Vorgangsweise wäre zB die Schaffung eines Zusatzprotokolls zum „Cybercrime-Übereinkommen" des Europarats: Darin könnten strafrechtliche Mindeststandards für Gewalt verherrlichende, rassistische uä Inhalte geschaffen werden; dies verbunden mit der Verpflichtung für die Vertragsstaaten, die Verbreitung solcher Inhalte unter Strafe zu stellen. Die globale Umsetzung solcher Mindeststandards dürfte aber auf Grund der unterschiedlichen (kulturellen) Wertesysteme und des in einigen (va in den angloamerikanischen) Staaten umfassenden Rechts auf freie Meinungsäußerung schwierig zu erreichen sein. Dennoch sollte als erster Schritt zumindest an einer kontinentaleuropäisch einheitlichen Regelung gearbeitet werden.