University of Zurich[UZH]

Zurich Open Repository and Archive
University of Zurich
University Library
Strickhofstrasse 39
CH-8057 Zurich
www.zora.uzh.ch

Year: 2008

Strafbare Handlungen im Internet - wer ist verantwortlich? Die fehlende gesetzliche Regelung in der Schweiz schafft Rechtsunsicherheit

Schwarzenegger, Christian

Posted at the Zurich Open Repository and Archive, University of Zurich
ZORA URL: https://doi.org/10.5167/uzh-17526
Journal Article

Originally published at:
Schwarzenegger, Christian (2008). Strafbare Handlungen im Internet - wer ist verantwortlich? Die fehlende gesetzliche Regelung in der Schweiz schafft Rechtsunsicherheit. Tangram, (21):52-56.

Strafbare Handlungen im Internet – Wer ist verantwortlich?

Die fehlende gesetzliche Regelung in der Schweiz schafft Rechtsunsicherheit

Christian Schwarzenegger

Am 3. August 2004 ging bei der Bundeskriminalpolizei eine Meldung aus Pakistan ein, welcher zufolge in einem Internetdiskussionsforum Terrorpropaganda veröffentlicht worden sei. Das Forum befand sich auf einem Schweizer Netzwerkcomputer. Eingerichtet hatte es ein tunesischer Asylant von seiner Wohnung im Kanton Fribourg aus. Die Ermittlungen ergaben, dass sich auf diesem und anderen Webforen des Mannes und seiner muslimischen Partnerin strafrechtlich relevante Gewaltdarstellungen, Aufforderungen zu Gewalttaten gegen Ungläubige, Anleitungen zur Herstellung von Sprengstoffen, Rassendiskriminierung und Hyperlinks auf Hinrichtungsvideos befanden. Die Informationen stammten aus dem Umfeld des Al-Qaida-Netzwerks, ihre Urheber oder Absender konnten nicht eruiert werden. Das Bundesstrafgericht hatte im Juni 2007 zu entscheiden, ob sich der angeklagte Asylant und seine Partnerin durch das Einrichten der Webforen strafbar gemacht hatten.

Viele Beteiligte an der Internetkommunikation

Die Urheber verbotener Informationen (Content-Provider) sind die Hauptverantwortlichen. Sie müssten an erster Stelle verfolgt werden. Doch diese Täter agieren irgendwo auf der Welt, sind mobil und können selten identifiziert werden. Weil Kommunikation im Internet oder in Mobilfunknetzen ohne Infrastruktur und softwaregesteuerte Dienste nicht funktioniert, kommt auch eine Strafbarkeit der weiteren Beteiligten in der Kommunikationskette in Betracht (siehe Abbildung, S. 54). Seit über zehn Jahren streiten sich Juristen und Praktiker darüber, wer für strafbare Handlungen im Internet und in anderen Netzwerken zur Rechenschaft gezogen werden soll.

Viele offene Fragen

Ohne Provider gibt es keine illegale Kommunikation. Es überrascht daher nicht, wenn eine Strafbarkeit aller Beteiligten gefordert wird. Nach dem Strafgesetzbuch sind die Antworten aber unklar. Um die Meinungsfreiheit nicht zu beeinträchtigen, sieht das Strafgesetzbuch bei Veröffentlichungen in einem Medium eine Beschränkung der Strafbarkeit vor. Alleine der Autor soll bestraft werden. Nur wenn dieser nicht zu fassen ist, wird subsidiär ein für die Publikation Verantwortlicher bestraft. Unklar ist nun, ob die Sonderregelung auch auf Veröffentlichungen im Internet anwendbar ist, ob die Provider straffrei bleiben und welche Delikte betroffen sind. Das Bundesstrafgericht erklärte sie im Beispielfall kurzerhand für nicht anwendbar. Der «Täter» hatte auf seiner Website nur ein inhaltsloses Webforum eingerichtet. Die illegalen Informationen wurden von Dritten erst später darin abgespeichert. Hat der Mann überhaupt eine strafbare (aktive) Handlung begangen? Oder hat er es unterlassen, etwas gegen die illegalen Inhalte zu unternehmen, nachdem er sie sah? War er strafrechtlich verpflichtet, den weiteren Abruf der Daten zu verhindern (Garant)? Wäre er dann Täter oder Gehilfe? Hat er sich die fremden Informationen zu eigen gemacht, das heisst die Verantwortung für sie übernommen? Die strafrechtliche Doktrin ist in diesen Fragen gespalten. Die Gerichte entscheiden einmal so, einmal anders. Klare Lösungen sind von der Rechtsprechung nicht zu erwarten. Vielmehr müssen die Provider in einem rechtsunsicheren Umfeld operieren, welches sie in der Entfaltung ihrer Dienstleistungen hemmt.

Gesetzliche Regelung notwendig

Die Expertenkommission «Netzwerkkriminalität»[1] schlug 2003 eine Neuregelung vor. Das Medienstrafrecht sollte für Presse,

Radio und Fernsehen unverändert bleiben. Der Vorschlag stellte weiterhin klar, dass Access-Provider nicht für die Informationen, zu denen sie den Zugang eröffnen, strafrechtlich verantwortlich sind. Parallele Strafbarkeitsgrenzen gelten gemäss E-Commerce-Richtlinie seit 2000 auch in den Mitgliedsstaaten der EU. Einer besonderen Regelung sollten Host-Provider und Suchmaschinenbetreiber unterstehen. Der Entwurf entkoppelte die Voraussetzungen der Strafbarkeit dieser Provider von den strafbaren Handlungen der Content-Provider. Diese Lösung hätte den Vorteil geboten, dass Host-Provider und Suchmaschinenbetreiber einheitlich nur wegen Nichtverhinderns einer strafbaren Handlung in elektronischen Kommunikationsnetzen hätten strafbar werden können, und zwar nur bei sicherem Wissen über die illegalen Inhalte.

Konsens in der Sache – Meinungsunterschiede im Detail

Die Vorschläge wurden im Oktober 2004 in die Vernehmlassung geschickt. Aus den zahlreichen Antworten liess sich der klare Konsens entnehmen, dass eine Klärung der Rechtslage durch den Gesetzgeber erforderlich sei. Die Kritik konzentrierte sich auf die Einführung einer Strafbarkeit des Host-Providers, insbesondere bei einem Verstoss gegen die Weiterleitungspflicht an die Strafverfolgungsbehörden. Eine völlige Straffreistellung wäre jedoch nicht sinnvoll. Host-Provider haben eine vertragliche Beziehung mit dem Content-Provider, und sie haben Kontrolle über den Webserver. Es kann von ihnen zwar nicht verlangt werden, aktiv nach illegalen Informationen zu suchen. Sobald sie aber von diesen sichere Kenntnis haben, müssen sie reagieren. In Deutschland, Österreich und England reicht die Kenntnisnahme eines Hinweises aus, um die Sperrpflicht aus-

Infobox

Drei internationale Instrumente gegen Kriminalität und Rassismus im Internet

Europäische Kommission gegen Rassismus und Intoleranz (ECRI):

Empfehlung No. 6, Dezember 2000: «La Lutte contre la diffusion de matériel raciste, xénophobe et antisémite par l'internet»

Inhalt: Rassismus ist in den Kampf gegen Internetkriminalität einzubeziehen; Sensibilisierung der Strafverfolgungs- und Gerichtsbehörden auf das Thema Rassismus; Sensibilisierung der Gesellschaft bezüglich dieser Thematik; Förderung antirassistischer Initiativen auf dem Netz; Klärung der Verantwortlichkeit der Provider; Unterstützung von Selbstregulierungsmechanismen der im Internet tätigen Unternehmen.[1]

Internationales Abkommen über die Cyber-Kriminalität

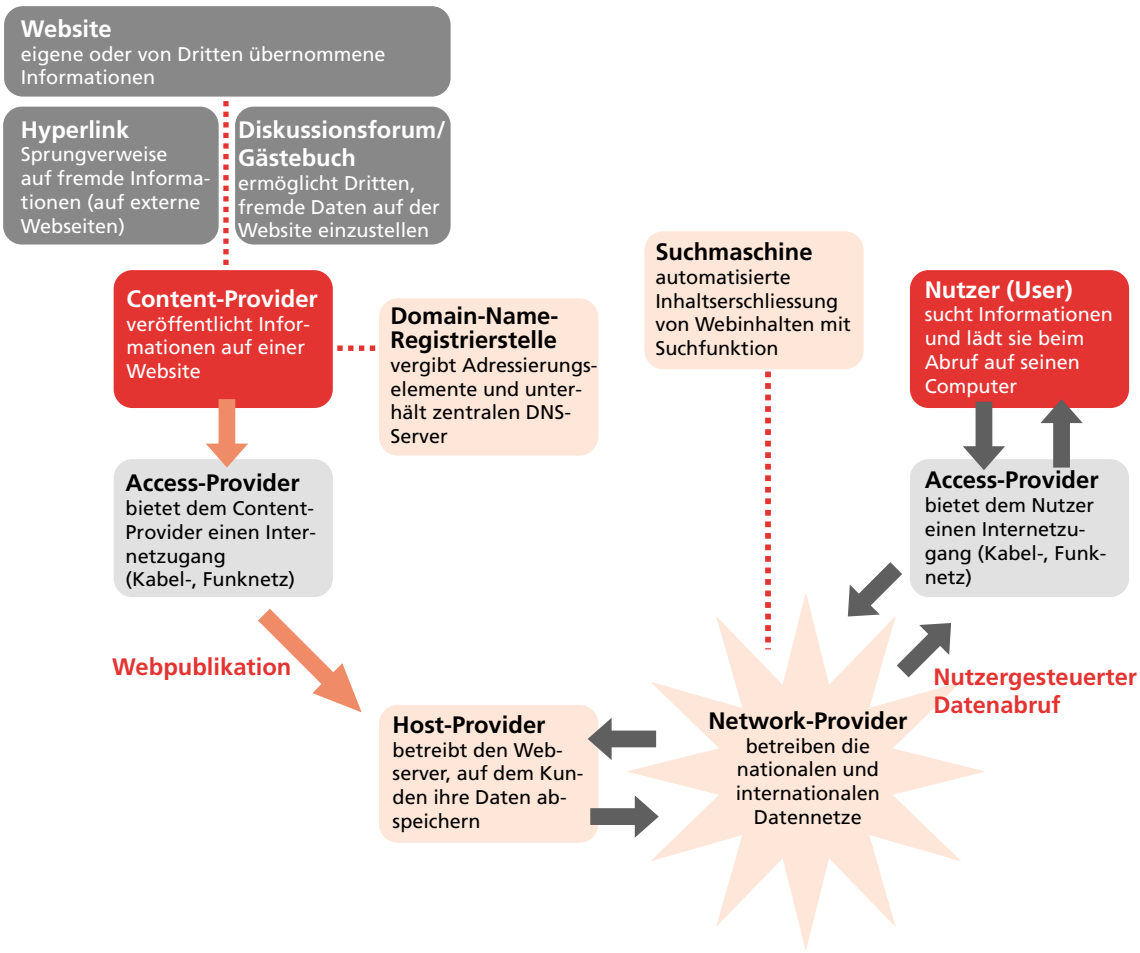
In Kraft seit dem 1. Juli 2004, heute von 22 Staaten ratifiziert. 2001 von der Schweiz unterschrieben, Ratifizierung in naher Zukunft vom Bundesrat geplant. Inhalt: Klärung der Rechtsbegriffe und der Fragen des Datenschutzes, des Datenzugriffs und der Verantwortlichkeit. Internationale Standards zur Bekämpfung von Internetkriminalität.[2]

Zusatzprotokoll zum Abkommen über die Cyber-Kriminalität

2003 genehmigte der Bundesrat das Zusatzprotokoll zum Abkommen über die Cyber-Kriminalität, das für die Mitgliedsstaaten des Europarats einen vergleichbaren Standard für die Rassismusbekämpfung im Internet schafft. Das Zusatzprotokoll führt rechtliche Massnahmen ein, um rassistisch motivierte, über einen Computer begangene Taten unter Strafe zu stellen, insbesondere das Verbreiten von rassistischem Material, die öffentliche Beleidigung aufgrund rassistischer Motive sowie das Leugnen und Verharmlosen von Völkermord. Eine Anpassung von Art. 261bis StGB war nicht notwendig. Das Zusatzprotokoll verweist auf die prozessrechtlichen Bestimmungen und die Grundsätze der internationalen Zusammenarbeit, die im Abkommen über die Cyber-Kriminalität enthalten sind.[3]

[1] *www.coe.int/t/e/human_rights/ecri/1-ecri/3-general_themes/1-Policy_Recommendations/_intro.asp*
[2] *S. auf der Website des Europarats: http://conventions.coe.int/Treaty/Commun/ListeTraites.asp?MA=49&CM=7&CL=GER*
[3] *S. Niggli, Marcel Alexander, Rassendiskriminierung, Ein Kommentar zu Art. 261bis und Art. 171c MstG, 2. Auflage, Zürich, 2007, S. 641-656. S. die Pressemitteilung des EJPD, 19.09.2003: http://www.bj.admin.ch/bj/de/home/dokumentation/medieninformationen/2003/22.html*

Die an der Kommunikation im World Wide Web Beteiligten und ihre Funktion



zulösen. Anders der Vorschlag für die Schweiz: Hier sollte die Strafverfolgungsbehörde zur Klärung der Situation eingeschaltet werden. Erst wenn diese den Host-Provider über die Eröffnung eines Strafverfahrens informiert, wäre eine Sperrung zwingend geboten. Eine seriöse Abklärung der Strafbarkeit ist Aufgabe der Strafverfolgungsbehörden und nicht der Host-Provider.

Ablehnende Haltung des Bundesrates – Umsetzung durch parlamentarische Initiative?

Trotz ausgewiesenen Regelungsbedarfs hat der Bundesrat am 28. Februar 2008 entschieden, diese Regelung der strafrechtlichen Verantwortlichkeit nicht weiterzuverfolgen.[2] Stattdessen wurden in der Botschaft zur Änderung des Bundesgesetzes über Massnahmen zur Wahrung der inneren Sicherheit sektorielle Regelungsvorschläge vorgebracht: Löschungsverfügungen gegen Host-Provider und (unverbindliche) Sperrempfehlungen an Access-Provider bei Propaganda-Aktionen. Eine umfassende und klare Regelung der strafrechtlichen Verantwortlichkeit der Provider in elektronischen Kommunikationsnetzen ist aber nach wie vor notwendig. Es überrascht daher nicht, dass nun im Nationalrat eine parlamentarische Initiative eingereicht wird, welche die Anpassung des Strafrechts an die Informationsgesellschaft direkt umzusetzen versucht.

Christian Schwarzenegger ist Professor für Strafrecht, Strafprozessrecht und Kriminologie an der Rechtswissenschaftlichen Fakultät der Universität Zürich und war Vizepräsident der Expertenkommission Netzwerkkriminalität (2002-2004). christian.schwarzenegger@rwi.uzh.ch

[1] Eidgenössisches Justiz- und Polizeidepartement (Hrsg.), Netzwerk-Kriminalität, Bericht der Expertenkommission, Bern 2003/2004

[2] Bundesrat, Netzwerkkriminalität, Strafrechtliche Verantwortlichkeit der Provider, Bericht des Bundesrates, Bern 2008

Qui est responsable en cas de cybercriminalité?

La difficulté, lorsqu'il s'agit de punir des infractions pénalement répréhensibles commises sur Internet ou sur d'autres réseaux de communication, réside dans le fait que les auteurs des informations illicites opèrent à partir de quelque part dans le monde et peuvent rarement être identifiés. On réfléchit depuis longtemps à la possibilité de poursuivre pénalement les autres acteurs de la Communication en réseau. La Commission d'experts «Cybercriminalité» a proposé en 2003 de ne rien changer à la législation en matière de droit des médias pour la presse, la radio et la télévision. Par ailleurs, selon la commission, les fournisseurs d'accès ne doivent pas assumer la responsabilité pénale des informations auxquelles ils donnent accès. Une réglementation particulière devrait par contre être appliquée aux fournisseurs d'hébergement et aux exploitants de moteurs de recherche, car les premiers ont une relation contractuelle avec les fournisseurs de contenus et, par conséquent, un contrôle sur les serveurs web. Toujours selon les experts, les fournisseurs d'hébergement ne doivent pas effectuer activement la recherche d'informations illicites, en revanche, en cas de «connaissance sûre», ils sont obligés de réagir. L'autorité de poursuite pénale doit clarifier la situation, mais avant d'ordonner le blocage du site, elle est tenue informer le fournisseur d'hébergement qu'une poursuite pénale a été est ouverte à son encontre. Bien qu'il soit nécessaire d'édicter une réglementation en la matière, le Conseil fédéral a décidé le 28 février 2008 de ne pas donner suite aux propositions de la commission d'experts. Dans son message, il proposait plutôt des réglementations sectorielles, telles que des décisions de suppression du site à l'encontre du fournisseur d'hébergement et une recommandation (non contraignante) de blocage du site à l'encontre du fournisseur d'accès en cas d'actes de propagande. On tente de mettre directement en œuvre l'adaptation du droit pénal à la société de l'information au moyen d'une initiative parlementaire déposée au Conseil national.

Christian Schwarzenegger est professeur de droit pénal, de droit de la procédure pénale et de criminologie à la Faculté des sciences juridiques de l'Université de Zurich; il a été vice-président de la Commission d'experts cybercriminalité. christian.schwarzenegger@rwi.uzh.ch

I n f o b o x

Trois instruments internationaux pour lutter contre la cybercriminalité et le cyberracisme

Commission européenne contre le racisme et l'intolérance (ECRI):

Recommandation N° 6, décembre 2000: «La Lutte contre la diffusion de matériel raciste, xénophobe et antisémite par l'Internet»

Teneur: intégrer le racisme dans la lutte contre la cybercriminalité; sensibiliser les autorités de poursuite pénale et judiciaires sur le thème du racisme; sensibiliser la société sur toutes les questions concernant cette thématique; soutenir les initiatives contre le racisme existant sur Internet; clarifier la responsabilité encourue par les fournisseurs d'hébergement; soutenir les mesures d'autodiscipline prises par l'industrie de l'Internet.[1]

Convention internationale contre la cybercriminalité

En vigueur depuis le 1er juillet 2004, ratifiée à ce jour par 22 Etats. Signée par la Suisse en 2001, ratification prévue dans un avenir proche par le Conseil fédéral.

Teneur: clarifier les notions juridiques et les questions relevant de la protection des données, de l'accès aux données et de la responsabilité. Définir des normes internationales pour lutter contre la cybercriminalité.[2]

Protocole additionnel à la Convention contre la cybercriminalité

En 2003, le Conseil fédéral a approuvé le protocole additionnel à la Convention contre la cybercriminalité qui oblige les Etats membres du Conseil de l'Europe à adopter des normes équivalentes pour lutter contre le racisme sur Internet. Ce protocole introduit des mesures juridiques permettant d'ériger en infraction pénale les actes obéissant à des motivations racistes qui sont commis au moyen des systèmes informatiques, notamment la diffusion de matériel raciste, les insultes à caractère raciste et la négation ou la minimisation du génocide. Il n'a pas été nécessaire d'adapter l'article 261bis CP. Le protocole additionnel renvoie aux dispositions du droit de procédure et aux principes de coopération internationale figurant dans la Convention.[3]

[1] *http://www.coe.int/t/e/human_rights/ecri/1-ecri/3-general_themes/1-Policy_Recommendations/_intro.asp*
[2] *http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=185&CM=8&DF=4/17/2008&CL=FRE*
[3] *S. Niggli, Marcel Alexander, Rassendiskriminierung. Ein Kommentar zu Art. 261bis und Art. 171c MstG, 2. édit., Zurich, 2007, p. 641-656. Voir le Communiqué de presse du DFJP, 19.09.2003: http://www.bj.admin.ch/bj/fr/home/dokumentation/medieninformationen/2003/22.html et le Protocole additionnel:http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=189&CM=8&DF=4/17/2008&CL=FRE*

I n f o b o x

Tre strumenti internazionali contro la criminalità e il razzismo in Internet

Commissione del Consiglio d'Europa contro il razzismo e l'intolleranza (ECRI):

Raccomandazione n. 6, dicembre 2000: «La lutte contre la diffusion de matériel raciste, xénophobe et antisémite par l'internet»
Contenuti: necessità di includere il razzismo nella lotta alla cibercriminalità; sensibilizzazione delle autorità giudiziarie e di perseguimento penale sul tema del razzismo; sensibilizzazione generale della società sull'argomento; promozione di iniziative antirazziste sulla rete; precisazione delle responsabilità dei provider; sostegno ai meccanismi di autoregolamentazione delle imprese operanti su Internet[1].

Convenzione del Consiglio d'Europa sulla cibercriminalità
In vigore dal 1°luglio 2004, la convenzione è finora stata ratificata da 22 Stati. Nel 2001 è stata firmata anche dalla Svizzera, che prevede di ratificarla in un prossimo futuro.
Contenuti: definizione dei concetti giuridici e spiegazione degli aspetti di protezione dei dati, accesso ai dati e responsabilità; standard internazionali di lotta alla cibercriminalità.[2]

Protocollo addizionale alla Convenzione sulla cibercriminalità
Nel 2003 il Consiglio federale ha approvato il Protocollo addizionale alla Convenzione sulla cibercriminalità, che, per gli Stati membri del Consiglio d'Europa, istituisce norme comparabili per la lotta al razzismo diffuso via Internet. Il Protocollo addizionale contro il razzismo e la xenofobia prevede una pena per atti commessi con motivazioni razziste e per mezzo di un sistema informatico, in particolare la divulgazione di materiale a sfondo razzista, l'offesa pubblica per motivi razzisti, nonché la negazione e la minimizzazione di genocidi. Non è stato necessario adeguare l'articolo 261bis del Codice penale svizzero. Il Protocollo addizionale rinvia inoltre alle disposizioni procedurali e ai principi di cooperazione internazionale contenuti nella Convenzione sulla cibercriminalità[3].

[1] http://www.coe.int/t/e/human_rights/ecri/1-ecri/3-general_themes/1-Policy_Recommendations/_intro.asp
[2] http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=185&CM=8&DF=4/17/2008&CL=ITA
[3] Niggli, Marcel Alexander, Rassendiskriminierung. Ein Kommentar zu Art. 261bis und Art. 171c MstG, 2a ed., Zurigo, 2007, pagg. 641-656. Cfr. comunicato stampa DFGP, 19.09.2003: http://www.bj.admin.ch/bj/it/home/dokumentation/medieninformationen/2003/22.html e Protocollo addizionale: http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=189&CM=8&DF=4/17/2008&CL=ITA

Reati commessi in Internet: a chi la responsabilità?

La difficoltà di perseguire i reati commessi in Internet e su altre reti di comunicazione elettronica è dovuta al fatto che gli autori dei contenuti illeciti operano da qualche parte nel mondo e raramente riescono a essere identificati. Da diverso tempo si sta pertanto riflettendo sull'opportunità di procedere penalmente contro gli altri partecipanti al processo comunicativo. Nel 2003, la commissione peritale «Criminalità in rete» ha proposto di lasciare invariato il diritto penale in materia di stampa, radio e televisione.

Inoltre, secondo la commissione, i fornitori di accesso (access provider) non devono essere tenuti ad assumere la responsabilità per le informazioni a cui danno accesso. Agli hosting provider deve invece essere applicata una regolamentazione speciale dato che hanno un rapporto contrattuale con i fornitori di contenuti (content provider) e quindi un controllo sui propri server. Sempre secondo la commissione peritale, gli hosting provider non devono procedere attivamente alla ricerca di contenuti illeciti ma, qualora ne siano a conoscenza con certezza, hanno il dovere di reagire. Le autorità di perseguimento penale hanno il compito di accertare la situazione, ma prima di ordinare la chiusura di un sito devono informare l'hosting provider del procedimento penale aperto nei suoi confronti. Nonostante la necessità di disciplinare la questione, il 28 febbraio 2008 il Consiglio federale ha deciso di non dare seguito alle proposte della commissione peritale, sostituendole – in sede di messaggio – con un progetto di regolamentazione settoriale, che contempla, fra l'altro, la possibilità di emanare decisioni di cancellazione dei contenuti all'indirizzo degli hosting provider e raccomandazioni (non vincolanti) destinate ai fornitori di accesso per il blocco di siti in caso di azioni di propaganda. Mediante un'iniziativa parlamentare depositata in Consiglio nazionale si cerca di applicare direttamente alla società dell'informazione l'adeguamento del diritto penale.

Christian Schwarzenegger, professore di diritto penale, diritto processuale penale e criminologia presso la facoltà di scienze del diritto dell'Università di Zurigo e vicepresidente della commissione peritale «Criminalità in rete» (2002-2004). christian.schwarzenegger@rwi.uzh.ch