HUMBOLDT FORUM RECHT
- Die juristische Internet-Zeitschrift an der Humboldt-Universität zu Berlin -

HFR 4/2009 ISSN 1862-7617 Aufsatz

Professor Dr. Rolf H. Weber und Romana Weber, Zürich

International ordre public for terrorism-related Internet content?*

Existing measures are not sufficient to satisfactorily combat the dissemination of illegal con-tent on the internet. Therefore, the existing international Conventions on terrorism need to be concretized and measures to have to be found to effectively implement and enforce them. The fact that terrorism merits to be prohibited is commonly acknowledged and constitutes part of international ordre public. Terrorist acts violate human rights, in particular the right to life as one of the most fundamental human rights. If the security interests outweigh the individual's rights to freedom of speech or open communication in particular case, the illegal information has to be removed from the internet. However, not only repressive, but also preventive actions need to be taken. Preventive efforts can consist in the introduction of technological barriers, the threat for Internet providers of being held liable or the threat for nation states of being sanctioned for not complying with their obligations.

I. Introduction

1 The global nature of the Internet and the ease of access make it a premium medium for the dissemination of information. The various information channels allow the distribution of legal, but also of illegal contents. This problem is aggravated by the fact that activities can be carried out in the online world by an unprecedented speed and degree of anonymity. Dissemination proceeds cheaply and effortlessly without a high risk of prosecution due to the chaotic structure of the Internet and due to the fact that "traces" of cybercommunications can be easily hidden. Furthermore, Western democratic states have up to now been strongly resisting to national control measures because of the high value given to the freedom of speech[1].

2 Through the Internet, the public can be very easily reached directly. The Internet offers the possibility to broadcast illegal content worldwide, uncensored and unfiltered. Chat rooms, websites and bulletin boards are largely uncontrolled, only few filters have been established[2].

3 With regard to terrorism, it is particularly data mining, planning and coordination, instructions and online manuals, terrorist propaganda and threats, recruitment, training and mobilization as well as fundraising and financing that takes place on the Internet. Furthermore, the Internet also serves as platform for attacking other terrorists[3]. Such

* Der Aufsatz wurde im Rahmen des 7. Beitragswettbewerbes "Recht in Zeiten des Terrors" angefertigt. Rolf H. Weber is chair professor for Private, Business and European Law, Director at the Center for Information and Communication Law at the University of Zurich Faculty of Law and Attorney-at-Law in Zurich. Romana Weber, lic. iur., is research assistant at the University of Zurich Faculty of Law and a Ph.D. student. The authors would like to thank Prof. Christine Kaufmann, University of Zurich, for her valuable comments and inputs.

[1] GABRIEL WEIMANN, Online Terrorism – Modern Terrorists and the Internet, in: GLAAB (ed.), Medien und Terrorismus – Auf den Spuren einer symbiotischen Beziehung, Berlin 2007, 51-58, at 51-52; STEPHAN ALEXANDER WEICHERT, Die Propaganda der Tat – Zur Kommunikationsstrategie des modernen Aufmerksamkeitsterrorismus, in: GLAAB (ed.), Medien und Terrorismus – Auf den Spuren einer symbiotischen Beziehung, Berlin 2007, 83-98, at 94-95; ROLF H. WEBER, Regulatory Models for the Online World, Zurich 2002, at 190.

[2] WEIMANN (fn. 1), at 54.

[3] For further explanations on the uses of the Internet by terrorists see GABRIEL WEIMANN, Terror on the Internet, Washington 2006, at 111-145; STEPHEN M. FURNELL/MATT J. WARREN, Computer Hacking and Cyber Ter-

kind of information can be considered illegal, as it supports the undertaking of terrorist actions, which violate human rights, in particular the right to life and health[4]. For information to be considered illegal having the consequence that a prohibition of dissemination would prevail the right to freedom of speech and open communication[5], an actual or potential threat for the society must be established. While the presentation of terrorist views, propaganda or fundraising and financing do not constitute an immediate danger to human life or health, they contribute significantly to the execution of terrorist attacks. This indirect threat is sufficient to shed light on the issue of a balancing of interests.

S. 53

4 The dissemination of illegal content is prohibited by most national criminal laws, irrespective of the carrier of the information. However, bearing in mind the global dimension of the Internet, individual states do not have sufficient power and resources to effectively tackle the problem of the dissemination of illegal terrorist information. International co-operation mechanisms should improve the fight against terrorism; other means are the development of new forms of self-regulation, the public-private "co-regulation", as well as national instruments for removing and blocking illegal content. If mechanisms for international co-operation are established, states can operate across borders, thereby benefiting from experiences of other states in their own implementation and enforcement of rules[6].

5 **II. Content-related regulation**

1. Problem of common understanding

While current international harmonization mainly attempts to protect fundamental rights, achieving agreements on the limits of these rights has proved to be much more difficult. Establishing a common understanding of illegal content in the Internet is challenging as different standards are applied by various users and legislators. Political, historical, religious and social considerations lead to different understandings. Furthermore, reality shows that the persons concerned often react differently depending upon their view of the situation. Not everybody finds the same degree of information offending, or shows the same sensitivity in respect of civility and cultural integrity. Nevertheless, in some critical areas the development of a common understanding can be observed disregarding any political maneuvers; some basic issues of civility are not really in dispute. Accordingly, at the Stockholm gathering in 2000, where 700 delegates from 46 countries participated, European leaders such as Germany's former Chancellor Gerhard Schröder and Switzerland's former Federal Councillor Ruth Dreifuss warned that the Internet should not become a cross-border vector for racist theories fomenting hate and discrimination[7].

6 Up to now, an international consensus exists only to a limited extent on issues such as racism, obscenity, discrimination or hate[8]. However, a positive tendency towards a change of this practice can be observed concerning terrorism which eventually may lead to an agreement within the international community stating that the restriction of

---

rorism: The Real Threats in the New Millenium?, Computers and Security, Vol. 18, 1999, 28-34, at 29; FRED COHEN, Terrorism and Cyberspace, Network Security, Vol. 5, 2002, 17-19, at 18-19.

[4] COUNCIL OF EUROPE, Cyberterrorism – The Use of the Internet for Terrorist Purposes, Strasbourg 2007, at 33-38.

[5] Article 10 of the European Convention on Human Rights.

[6] The need to counter the terrorist use of the Internet was also articulated by the Council of Europe, COUNCIL OF EUROPE, Internet – A Critical Resource for All, Document presented by the Secretary General of the Council of Europe to the Internet Governance Forum, Hyderabad, India, 3-6 December 2008, at 13; HELEN KELLER, Expertenpanel: Freiheit durch Sicherheit ohne Freiheit – Die Problematik der Terrorismusbekämpfung, in: KIRCHSCHLÄGER ET AL. (eds), Menschenrechte und Terrorismus, 1. Internationales Menschenrechtsforum Luzern (IHRF), Bern 2004, 145-147, at 145.

[7] WEBER (fn. 1), at 190.

[8] United Nations World Conference on Racism, Racial Discrimination and Xenophobia in late 2001; WEBER (fn. 1), at 190-191 and 194-195.

freedom of speech (amongst other human rights) is justified in order to take action against the dissemination of terrorist information on the Internet.

S. 54

7 So far, no universally accepted definition of the term "terrorism" is available. In this contribution, terrorism will refer to movements pursuing political, religious or ideological goals. Accordingly, these movements have a public character. Furthermore, terrorist actions use the exercise or threat of violence against humans or propriety to achieve their goals; their aim is to succeed in their protest by intimidation or exercise of pressure on other individuals[9].

8 During the last few years, a broad consensus has emerged that terrorist actions are illegal. In case of terrorist attacks, various human rights are violated and innocent people hurt. Furthermore, if terrorists act internationally, they intrude into the territory of sovereign states. The respective acts cannot be justified, which makes them illegal considering their consequences. The fight against terrorism also serves the protection of securing peace by a legally established co-operation of states[10].

9 Furthermore, a common understanding has evolved that terrorism must be fought. This acknowledgement asks for repressive as well as preventive measures. On the one hand, the dissemination of new terrorist information on the Internet needs to be prevented; mechanisms have to be put in place which control the relevant information made available online and which have the power to prohibit certain information from being made accessible to all users. On the other hand, illegal terrorist material already available in the Internet has to be discovered and removed. Considering the enormous amount of information available on the Internet, such a task is challenging, in particular because illegal information is often hidden. However, with the help of all users of the Internet, the goal of removing illegal terrorist content can be realized to a far extent.

10 In general, efforts to establish principles of a common understanding are worth supporting since restraints on commonly unwanted issues could also help to achieve political appeasement[11].

11 **2. Rulemaking approaches**

Tackling the problem of dissemination of illegal terrorist content on the Internet requires specific regulations based on research related to technical blocking and control mechanisms on the Internet. These regulations must take into consideration the consequences of such measures for human rights, in particular freedom of speech.

S. 55

12 ***2.1 Government regulation***

Traditional government regulation is usually the first reaction to an undesired social development; this approach has also been chosen as regards illegal content on the Internet. Most countries have either passed special laws protecting citizens or certain parts of the population, for example minors, against different forms of undesirable content, or have at least amended existing laws. However, from a legal and practical perspective, success has been rather limited. Discrepancies between fundamental rights

[9] For an approach of a definition of terrorism see ROLF H. WEBER/ROLAND UNTERNÄHRER, Wirtschaftsterrorismus im Internet, in: ACKERMANN/DONATSCH/REHBERG (eds), Wirtschaft und Strafrecht, Zurich 2001, 365-380, at 366-368; WEIMANN (fn. 1), at 21-22; PETER J. VAN KRIEKEN, Terrorism and the International Legal Order, The Hague 2002, at 13-20; JEAN-CHRISTOPHE MARTIN, Les Règles Internationales Relatives à la Lutte Contre le Terrorisme, Bruxelles 2006, at 35-69; ANTONIO CASSESE, International Criminal Law, 2nd edition Oxford 2008, at 166-169.

[10] HANS-JOACHIM HEINTZE, Das Völkerrecht wird unterschätzt, Internationale Politik und Gesellschaft, Vol. 3/2004, 38-60, at 43; CASSESE (fn. 9), at 163-165.

[11] WEBER (fn. 1), at 190-191.

and desired restrictions on free speech become even more cumbersome if the terms used in the respective legal provisions are vague and difficult to define satisfactorily[12].

13 The major disadvantage of traditional government regulation consists in its restricted territorial applicability. National cyber-policies have only a limited impact since they do not lead to a global approach. Because an international agreement does not exist regarding reasonable content regulation on the Internet, a geographically limited approach fails to have a widespread effect[13]. Even if adequate regulation of illegal Internet content does exist, enforcement of the respective norms can be hampered with difficulties, in particular in countries with weak judicial systems.

14 Furthermore, balancing different interests or applying the „proportionality test" only lead to very vague determination of doubtful activities and consequently remain open to different understandings under varying social and cultural circumstances which makes a uniform application of regulations concerning illegal content unlikely, even if an international consensus can be assumed to exist concerning terrorist information[14]. This fact causes different interpretations of various countries concerning the prohibition of illegal terrorist content on the Internet, preventing a general fight against the dissemination of particular information.

15 ***2.2 International agreements***

International agreements establish a common understanding of the member states regarding a specific topic. International regulation is more adapted to the global nature of the Internet than domestic regulation as it is not territorially bound. Furthermore, it defines the elements of an offence in a way obliging the international community, whereas state regulations often vary from one another in specific definitions[15].

S. 56

16 However, the preparation and incorporation of international agreements usually takes several years. Because the problem of terrorism flourishes by using the Internet as a platform, though, cross-border rules need to be established as promptly as possible. Generally looking, the international community has issued various calls in different legal formats for the suppression of terrorism[16]. Nevertheless, they are all based upon the idea of criminal law having a preventive character on the individuals to commit a

[12] WEBER (fn. 1), at 191; for examples of national legislation see also HELEN KELLER, Nach dem 11. September 2001 – Terrorismusbekämpfung als Herausforderung des Rechtsstaates, in: KAPPEL/TOBLER/WALDMANN (eds), Rechtsstaatlichkeit im Zeitalter der Globalisierung, Freiburg i. Br. 2005, 255-280, at 256-270.
[13] WEBER (fn. 1), at 193.
[14] WEBER (fn. 1), at 193; KLAUS W. GREWLICH, Governance in "Cyberspace", The Hague/London/Boston 1999, at 286-288.
[15] GREWLICH (fn. 14), at 291.
[16] UN Convention on the prevention and punishment of crimes against internationally protected persons, including diplomatic agents (with resolution 3166 [XXVIII] of the General Assembly of the United Nations) of 14 December 1973, UN Convention against the taking of hostages of 17 December 1979, UN Convention for the suppression of terrorist bombs of 15 December 1997, UN Convention for the suppression of the financing of terrorism of 9 December 1999, UN Convention for the suppression of acts of nuclear terrorism of 14 September 2005, UN Convention on offences and certain other acts committed on board aircraft of 14 September 1963, UN Convention for the suppression of unlawful seizure of aircraft of 16 December 1970, UN Convention for the suppression of unlawful acts against the safety of civil aviation (with Final Act of the International Conference on Air Law held under the auspices of the International Civil Aviation Organization at Montreal in September 1971) of 23 September 1971, UN Convention on the physical protection of nuclear material of 26 October 1979, Protocol for the suppression of unlawful acts of violence at airports serving international civil aviation of 24 February 1988, UN Convention for the suppression of unlawful acts against the safety of maritime navigation of 10 March 1988, Protocol for the suppression of unlawful acts against the safety of fixed platforms located on the continental shelf of 10 March 1988, UN Convention on the Marking of Plastic Explosives for the Purpose of Detection of 1 March 1991, General Assembly Resolutions 49/60 of 9 December 1994 51/210 of 16 January 1997 concerning measures to eliminate international terrorism, Security Council Resolution 1267 of 15 October 1999, Security Council Resolution 1373 of 28 September 2001, Security Council Resolution 1540 of 28 April 2004; many agreements have also been concluded at a regional level, for a list of relevant Conventions see VAN KRIEKEN (fn. 9), at 20-22. Furthermore, the United Nations General Assembly appointed an Ad Hoc Committee to elaborate a comprehensive Convention on international terrorism.

particular crime and serving the purpose of ensuring that delinquents can be prosecuted. International agreements follow the same reasoning; they define the elements of criminal acts and oblige state members to punish offenders adequately or to extradite them[17]. While these agreements acknowledge that international co-operation is necessary to address terrorism, they do not provide for specific recommendations concerning this co-operation. Furthermore, the subject of these agreements is to fight terrorist acts in general; they do not provide for specific co-operation recommendations, nor do they contain references to the dissemination of terrorist content in particular.

17 In a new Convention, the subject of dissemination of terrorist content on the Internet would have to be addressed explicitly. A respective agreement would simplify the process of eliminating terrorist information from the Internet and prevent new illegal terrorist content from being uploaded online. In substance, such an international consensus would need to include a definition on what constitutes illegal content in general in order to justify measures eliminating such content as well as to serve as basis for the establishment of liability or sanctions. Furthermore, rules for establishing liability of Internet providers should also be harmonized in order to confront provider neglecting their obligations with sanctions supported by a large majority of states. Moreover, specific rules about the co-operation of states have to be included in international agreements. Co-operation entails the exchange of information[18], assistance in technical and administrative matters as well as joint movements to avoid appearance of illegal content in the Internet. The principles relating to international co-operation included in the Convention on Cybercrime of the Council of Europe[19] could be introduced into such a new Convention. Means of communication have to be established which are secure in transporting this information to other countries. The Internet is a particularly suitable framework for international co-operation as it is accessible from everywhere, enabling governments to examine specific websites and exchange thoughts as well as be active in eliminating illegal content at the same time. Nevertheless, from a realistic point of view, it seems rather unlikely that such a new Convention will be agreed upon by most states in the near future; therefore, other legal means need to be considered.

S. 57

18 ***2.3 Self-regulation***

Several self-regulatory mechanisms at different levels exist which can be used to overcome the deficiencies of other regulatory approaches. A reason for turning to self-regulation is that state regulations are often not flexible enough to adapt legislation to the fast-changing needs of the Internet community and the applicability of state laws is limited to their own territory[20].

19 Most self-regulatory mechanisms fall under the notion of "soft law". According to the traditional conception[21], soft law is not enforceable or creating liability for the violator, because soft law is not formally binding. Soft law is often used as a catchphrase for particular forms of social rules close to public international law. Although soft law is not legally binding, it nevertheless has a certain legal significance[22]. For example, the possibility exists that through the existence of soft law, the creation of according customary law and the codification thereof is prepared and encouraged[23]. Furthermore, courts can use soft law in the interpretation of formal legal sources[24].

[17] HEINTZE (fn. 10), at 44.
[18] See also MARTIN (fn. 9), at 362-375.
[19] Council of Europe, Convention on Cybercrime, done at Budapest on 23 November 2001.
[20] WEBER (fn. 1), at 195-196.
[21] KNUT IPSEN, Völkerrecht, 5th edition Munich 2004, at § 19 N 20.
[22] DANIEL THÜRER, Völkerrecht, 3rd edition Zurich 2007, at 124-125.
[23] IPSEN (fn. 21), at § 19 N 21.
[24] MARKUS KRAJEWSKI, Wirtschaftsvölkerrecht, Heidelberg 2006, at N 90.

20 Self-regulation[25] can be introduced through the issuance and private enactment of codes of conduct. The respective codes are established by parties active in a specific field and interested in achieving a particular goal, most often international organizations or non-governmental organizations (NGOs). They could incorporate guidelines on Internet content and protection measures against illegal content. Bodies responsible for the introduction of according codes, as well as for their implementation and enforcement, should be appointed. Furthermore, if these self-regulatory bodies hear from the occurrence of illegal content on the Internet, they should immediately take steps to remove the respective information. As cyberspace is a highly technical environment, bodies responsible for effective enforcement of codes of conduct need to have extensive knowledge about technical possibilities to avoid the dissemination of illegal content. Therefore, NGOs active in the field of Internet functioning would be appropriate for the task. The state legislator could encourage and support the implementation of a code of conduct by granting it legal recognition or by pursuing a concept of "regulated self-regulation" or "co-regulation"[26].

S. 58

21 Another approach consists in the introduction of self-classification and filter systems. Such technological mechanisms allow the users to apply appropriate selection criteria according to their own judgment[27]. However, terrorist information is illegal in general. Therefore, the user should not even be able to make that choice at all; the dissemination of the respective content has to be prevented in general, without differing according to various groups of users.

22 The implementation of Internet hotlines is a further possible method of self-regulation. Such mechanisms provide users with the opportunity to identify illegal or undesired Internet content by entering details about the location of a site into a form on a web page. The receiver of the message does not just act as a mailbox, but also as an identifier of problematic content. Moreover, the hotlines (1) forward the complaint to the respective authorities, (2) process the identification of the source of the content by evaluating the criticized content as legal or illegal (evaluation function), and (3) make the decision to inform other hotlines and/or service providers. Since hotlines can cooperate internationally more easily and effectively than state enforcement authorities, and since they offer users reliable and immediately responsive points of content, collaboration among hotlines is vital[28].

23 The problem of code-based regulation is that it leaves the control of access to whatever information to private persons, not a democratically legitimate government. However, the balancing of security interests against human rights should not be left to private institutions[29]. As the regulation thereof can interfere with government policies and consequently involve public interests, it should be the government itself or a suprana-

[25] The general advantages of self-regulation include efficiency, increased flexibility, better incentives for compliance, and reduced costs. The acceleration of technological and social developments may also point to an approach which uses soft-law instruments, voluntary agreements, and co-operative self-regulation (for further details see WEBER [fn. 1], at 83-84 and 198).
[26] WEBER (fn. 1), at 196.
[27] WEBER (fn. 1), at 196-197; JACK M. BALKIN/BETH SIMONE NOVECK/KERMIT ROOSEVELT, Filtern von Internet-Inhalten, Ein Best-Practices-Model, in: WALTERMANN/MACHILL (eds), Verantwortung im Internet – Selbstregulierung und Jugendschutz, Gütersloh 2000, 211-284, at 212-221; STUART BIEGEL, Beyond Our Control?, Confronting the Limits of Our Legal System in the Age of Cyberspace, Cambridge Massachusetts 2001, at 200-201; HARVARD LAW SCHOOL, Developments in the Law – The Law of Cyberspace, Harvard Law Review, Vol. 112, 1999, 1574-1704, at 1597-1603.
[28] WEBER (fn. 1), at 197-198; HERBERT BURKERT, Hotlines, in: WALTERMANN/MACHILL (eds), Verantwortung im Internet – Selbstregulierung und Jugendschutz, Gütersloh 2000, 285-344; see also <http://www.fsm.de/de/Beschwerdestelle>; as an example for an early hotline see the Dutch Meldpunt, <http://www.meldpunt-kinderporno.nl/en/>.
[29] LAWRENCE LESSIG, The Future of Ideas, New York 2001, at 17-99.

tional body that decides which contents are illegal[30].

24 The effectiveness of self-regulatory mechanisms varies considerably according to the existence of domestic organizational structures capable of implementing self-regulatory schemes[31]. Criticism of self-regulation generally focuses on the private regulator's lack of democratic legitimacy, a subversion of regulatory goals to business goals, and the inadequacy of enforcement measures in self-regulatory regimes. At the moment, there is not much experience to draw on with regard to self-regulatory measures for Internet content control. However, experiences with self-regulation in the traditional field of media control (printing and electronic media) are in many cases good, even though not always unproblematic. Still, it should not be overseen that traditional media and the Internet are used differently and therefore require different rules[32].

S. 59

25 Existing self-regulatory mechanisms applicable in respect of Internet content could be improved under various approaches. First and foremost, the acceptability of soft-law measures might increase if the technical environment was standardized and harmonized. Filtering and self-rating software should be easily accessible and applicable without requiring the user to be a technological expert. Market participants and/or their industry organizations are in a position to fulfill this requirement if they are prepared to give up the notion of single approaches[33].

26 A solution to the enforcement problem of self-regulatory codes of conduct does not exist. However, if the state legislator takes steps to improve self-regulation, the standing of such rules will improve, as the willingness of market participants to observe the rules does not necessarily need to be based on strict legal provisions[34]. Furthermore, information about according codes of conduct also needs to be disseminated at an international level. International organizations or NGOs with a broad access to the public are best equipped for this task. The involvement of the public is indispensable in order to achieve the elimination of illegal content on the Internet. Tips from citizens who have, by chance or on purpose, encountered illegal information are indispensable as professionals will not be able to eliminate all illegal information by themselves, the structure of the Internet is too complex and too much information is available online to have an oversight. However, this presupposes that the public is aware of the problem of illegal content on the Internet and of the institutions to which they should turn in case they discover according material.

S. 60

27 ## 3. Evaluation

The existing rulemaking approaches are not sufficient to ensure that terrorist information is not disseminated on the Internet. Further mechanisms need to be introduced in order to increase the protection of individuals from terrorist attacks, which are often prepared online.

28 Improvements have to be made in the sharing of information as well as in the allocation of tasks related to the control of the global cyberspace. Regulation of international co-operation needs to include the obligation of states to adapt their domestic legislation to the respective international standards and provisions concerning the establishment and maintenance of channels of communication between different states' competent agencies and services to facilitate the secure and rapid exchange of information.

---

[30] WEBER (fn. 1), at 202-203; LAWRENCE LESSIG, Tyranny in the Infrastructure: The CDA Was Bad – But PICS May Be Worse, Wired Magazine, July 1997.
[31] GREWLICH (fn. 14), at 269.
[32] WEBER (fn. 1), at 199-201; ANGELA CAMPBELL, Self-Regulation and the Media, Federal Communications Law Journal, Vol. 51, 1999, 711-772, at 768-772.
[33] WEBER (fn. 1), at 118-124 and 201, with further references.
[34] WEBER (fn. 1), at 202.

Spontaneous information should also be encouraged in case of unexpected events[35].

29 New, globally applicable, rules for national substantive law and national procedural law, regulations concerning international co-operation, as well as rules establishing public-private partnerships would increase international involvement in the fight against terrorism[36]. A need for action to deal with the dissemination of illegal content in the Internet exists in all four areas: (1) Rules on illegal Internet content as well as responsibility of Internet providers need to be harmonized in substantive criminal law; (2) sanctions, the admittance of evidence and data privacy should be harmonized in procedural law; (3) the necessity of administrative and judicial assistance requires mechanisms for international co-operation; and (4) public-private partnerships involve all interested parties in the fight against terrorism, including individuals, which leads to manifold inputs and a broader acceptance of taken deci61ons.

30 The regulations to be created would have to be sufficiently precise in order to ensure their uniform application by members. Only if states interpret their obligations in the same way, their joint efforts to eliminate the dissemination of illegal information will be successful. Furthermore, precision in the definitions is also necessary to ensure an adequate balancing of measures for the elimination of illegal content against the restrictions on individual freedoms. However, a common understanding of most states to establish a respective Convention is unlikely to be achieved soon. Therefore, the question is whether existing mechanisms in international law can be applied and/or further developed in order to prevent illegal terrorism-related information from being made available online.

S. 61

31 ## III. Application of international *ordre public*?

With terrorism being a major threat to international peace and security[37], fighting terrorism may be linked to the concept of *ordre public*.

32 ### 1. *Ordre public* in international law

1.1 Ordre public in general

Ordre public represents the fundamental elements underlying and unifying every legal system. It represents a social interest of the entire society and is derived from the cultural and moral foundation of a society. The basis of every society can be found in its *ordre public*; when individuals had no other choice than to unify in order to originate new forces, their "contrat social", as Jean-Jacques Rousseau[38] described the joining together, included the fundamental values that the *ordre public* represents.

33 *Ordre public* has a normative character on its own by representing a common understanding[39]. It is subject of possible changes and has to be adapted or modified according to current views and changing conditions[40].

34 Most commonly, the concept of *ordre public* is used by countries in national and private international law; even in these situations, reference to public international law is

[35] For the need of further co-operation see van KRIEKEN (fn. 9), at 7.
[36] See above II. 2.2; COUNCIL OF EUROPE (fn. 4), at 96-97; ULRICH SIEBER, Staatliche Regulierung, Strafverfolgung und Selbstregulierung: Für ein neues Bündnis zur Bekämpfung rechtswidriger Inhalte im Internet, in: WALTERMANN/MACHILL (eds), Verantwortung im Internet – Selbstregulierung und Jugendschutz, Gütersloh 2000, 345-432, at 395-399.
[37] Security Council Resolution 1368 of 12 September 2001.
[38] JEAN-JACQUES ROUSSEAU, The Social Contract and Discourses by Jean-Jacques Rousseau, translated with an Introduction by G. D. H. Cole, London/Toronto 1923, Livre I, Chapitre VI, para. 2, available at <http//oll.libertyfund.org/ title/638>; for a philosophic approach to the governing of the Internet see also ROLF H. WEBER/ROMANA WEBER, Social Contract for the Internet Community?, forthcoming.
[39] WERNER LEVI, The International Ordre Public, Revue de droit international de sciences diplomatiques et politiques, Vol. 72, 1994, 55-77, at 57-59.
[40] LEVI (fn. 39), at 77.

made. The international *ordre public* referred to in the given context must be distinguished from the *ordre public* of the private international law system and national *ordres publics*[41]. The existence of an *ordre public* in public international law was contested for many years; however, it is now accepted as part of an evolving international constitutional law[42]. In the framework of international public law, *ordre public* is the expression of fundamental values of the international community. Norms of the ordre public touch the interests of all states to a special degree[43].

S. 62

35 ***1.2 Delimitation of ordre public to other categories of norms in public international law***

Ordre public is not the same as *ius cogens*. While *ordre public* has a broad field of application covering the entire legal order, including and in particular spiritual and social goals, only the most fundamental human rights are considered to be *ius cogens*. For the same reasons, *ius cogens* is distinct to a general common understanding; while *ius cogens* is always also a common understanding, not all issues based on a common understanding represent *ius cogens* norms, but only the most fundamental ones.

36 *Ius cogens* is binding; deviations are not admissible. This fact, however, does not suggest that other standards included in the *ordre public* are not binding. The most basic human rights represent norms with *erga omnes* effect. This effect implies that all states have a legal interest in the protection of the underlying rights because of their fundamental value[44]. Adherence to norms with *erga omnes* effect is owed to the whole international community. The category of norms with *erga omnes* effect addresses the question of towards whom states are obliged to adhere to the respective norms.

37 The logic of the fact that a nation state is bound by an *erga omnes* obligation towards the international community leads to the conclusion that all states can take reprisals against other states violating a norm with *erga omnes* effect[45]. The difference of these norms to *ius cogens* is that deviations are permissible under specific circumstances[46].

38 Another distinction between *ius cogens* and *ordre public* can be seen in the rank of *ius cogens* and the intensity of the obligation of the respective human rights connected thereto. Deviations form *ius cogens* on a contractual basis are not permissible; *ius cogens* has an increased strength of validity[47].

39 ***1.3 Effects of ordre public***

Ordre public is a particularly useful concept in the field of international law, since legislation is often unable in creating laws to keep pace with the rapid growth of emerging interests. Neither national legislation nor a multilateral treaty nor customary law are suitable to provide for regulation within a short span of time. Therefore, *ordre public* is

---

[41] LEVI (fn. 39), at 56; JÜRGEN BASEDOW, Die Verselbständigung des europäischen ordre public, in: COESTER/MARTINY/GESSAPHE, Privatrecht in Europa Vielfalt, Kollision, Kooperation, München 2004, 291-319, at 295; for the influence of the international *ordre public* on the *ordre public* in of the private international law system and the national *ordre public* see ANDREAS SPICKHOFF, Der völkerrechtsbezogene ordre public, in: LEIBLE/RUFFERT (eds), Völkerrecht und IPR, Jena 2006, 275-303; RALF MICHAELS, Public and Private International Law: German Views on Global Issues, Journal of Private International Law, Vol. 4, 2008, 121-138.

[42] LEVI (fn. 39), at 59-66; JULIANE KOKOTT, Grund- und Menschenrechte als Inhalt eines internationalen ordre public, in COESTER-WALTJEN/KRONKE/KOKOTT (eds), Die Wirkungskraft der Grundrechte bei Fällen mit Auslandbezug, Berichte der deutschen Gesellschaft für Völkerrecht, Heidelberg 1998, 71-114, at 77.

[43] KOKOTT (fn. 42), at 77 and 82-83.

[44] *Barcelona Traction, Light and Power Co.* (Belgium v. Spain), judgment of 5 February 1970, ICJ Reports 1970, 3, para. 33.

[45] KOKOTT (fn. 42), at 87; however, in the *East Timor* judgment, the ICJ did not come to this conclusion, see *Case Concerning East Timor* (Portugal v. Australia), judgment of 30 June 1995, ICJ Reports 1995, 89. para. 29.

[46] For example in a state of emergency.

[47] KOKOTT (fn. 42), at 88.

adapted to protect fundamental values[48].

S. 63

40 Human rights are the field most developed within public international law and therefore represent the most important foundation for the recognition of an international *ordre public*. This reasoning is based on the many existing Conventions on human rights, the generally recognized obligation of states to protect human rights and the third-party effect of these rights[49].

41 With respect to human rights, the common interests of society comprise for example the concern about peacekeeping, the concern to prevent situations of floods of refugees or expensive humanitarian actions, the protection of human rights as factor for the legitimacy of the organized community of states or the recognition of the value of human dignity not only in the domestic sphere, but also abroad. Accordingly, human rights being part of the *ordre public* are norms, which, because of their particular importance and function with relation to the peacekeeping for the sake of all, have to outweigh other interests[50].

42 **2. Prohibition of terrorism as element of *ordre public*?**

The Internet as means of communication for terrorists has only recently become an item of discussion of global importance. Effective legal measures to encounter the situation do not yet exist; therefore, the concept of *ordre public* has so far not been consulted as basis for measures taken in order to prevent further terrorist acts.

43 ***2.1 Balancing human rights***

Tackling terrorism is in the interest of the whole society; it promotes peace for all and encourages economic development. The fight against dissemination of illegal terrorist content on the Internet contributes significantly to the achievement of the respective goals[51]. However, security interests have to be balanced against the limitation of certain human rights. Very often, innocent people are hurt in the context of terrorist attacks; these persons need to be protected, even if it means that the respective objective limits certain other rights generally recognized under international law.

S. 64

44 Attacks against innocent civilians do not respect their right to life and dignity and should outweigh other fundamental standards such as free speech, open communication or freedom of press. If the right to life and dignity is limited, the individuals concerned by this limitation of their rights will often not even be in the position to enjoy other human rights such as the freedom of speech. In general, three conditions have to be met in order to justify the limitation of the right to freedom of speech: (1) existence of a legal basis for the limitation, (2) the limitation aims at a legitimate goal, and (3) the measure is proportionate[52].

45 Whether the right to life serves as legal basis for the limitation of the right to freedom is controversially discussed. The German Federal Constitutional Court decided that the governmental forces were not allowed to fire off high-jacked airplanes[53]; such an ac-

[48] LEVI (fn. 39), at 70.
[49] KOKOTT (fn. 42), at 79-82; WALTER KÄLIN, Menschenrechtsverträge als Gewährleistung einer objektiven Ordnung, in: KÄLIN/RIEDEL/KARL/BRYDE/VON BAR/GEIMER, Aktuelle Probleme des Menschenrechtsschutzes, Heidelberg 1994, 9-48; see also CHRISTINE KAUFMANN, Globalisation and Labour Rights, Oxford 2007, at 230.
[50] KÄLIN (fn. 49), at 36.
[51] See also HELEN KELLER, Einschränkung der Menschenrechte zum Schutz der Menschenrechte: Folter in der Terrorismusbekämpfung, in KIRSCHLÄGER ET AL. (eds), Menschenrechte und Terrorismus, 1. Internationales Menschenrechtsforum Luzern (IHRF), Bern 2004, 175-188, at 176; KELLER (fn. 6), at 146.
[52] FRANÇOIS MOYSE, La liberté de l'expression et l'ordre public en droit européen, Annales du droit luxembourgeois, 15.2005, 2006, 57-71, at, at 57-62.
[53] Deutsches Bundesverfassungsgericht (German Federal Constitutional Court), 15 February 2006.

tion most certainly leads to the death of the passengers of the respective airplane[54]. However, human life is the vital basis of human dignity, constituting a topmost constitutional principle. Every individual possesses this dignity being a person, notwithstanding his/her characteristics, physical or mental condition, performance or social status. The state is prohibited from taking measures violating this right to human life and dignity. Moreover, the state even has the obligation to protect human life from attacks by third parties. According to the German Federal Constitution Court, it is plainly prohibited to governmental agencies to treat individuals in a way that would put their status as legal person in question. The fact that more lives are saved than destroyed if a high-jacked airplane is fired off, does not change the fact that a respective measure disregards the dignity of the affected persons, neither does the fact that the respective passengers may die anyway[55]. A respective measure can only be justified if simply persons involved in the terrorist attack are on board of the airplane. From this judgment, the conclusion can be drawn that the right to life is one of the most fundamental rights and therefore outweighs other human rights, such as the right to freedom of speech.

46 The goal to preserve human life and dignity is also a legitimate goal; the limitation of freedom of speech is reasonable and adequate to achieve this goal as the protection of human life is a preponderant imperative of public interest. Accordingly, the right to life and dignity could be considered more fundamental justifying restrictions of the freedom of speech, open communication or freedom of press. The protection of these fundamental values as part of the *ordre public* is a legitimate goal and allows for the limitation of the mentioned freedoms[56].

47 Other ways to get attention from governments and/or society exist which do not involve the destruction of lives and property, such as approaching governments, media etc. with ideas on the implementation of the goals of terrorists. There is no legitimate reason for terrorists not to use these mechanisms, and respective approaches would not infringe the *ordre public*.

S. 65

48 *2.2 International initiatives demonstrating the existence of a common understanding*

The high number of global and regional agreements[57] concerning terrorism shows the existence of an international consensus that terrorism as phenomenon needs to be addressed. While these agreements address terrorism itself, they include (even if only implicitly) the use of the Internet by terrorists as part of the whole movement. Evaluated from another perspective, agreements on illegal use of the Internet have also been concluded; in particular the Convention on Cybercrime of the Council of Europe[58] springs to mind. Combining the efforts of these two kinds of agreements would lead to the establishment of an international agreements of illegal use of the Internet by terrorist, demonstrating the international belief that terrorism and all activities related to the phenomenon need to be abolished.

49 The existence of a common understanding and the need for international co-operation was also laid out in "A Proposal for an International Convention on Cyber Crime and Terrorism" proposed by the Hoover Institution, the Consortium for Research on Information Security and Policy (CRISP), the Center for International Security and Cooperation (CISAC), and Stanford University. Considering the potentially grave consequences of cyber attacks, and "convinced that there is an emerging consensus regarding certain conduct that should be prosecuted as criminal, as well as regarding the need for

[54] Deutsches Bundesverfassungsgericht (German Federal Constitutional Court), 15 February 2006, para. 87.
[55] Deutsches Bundesverfassungsgericht (German Federal Constitutional Court), 15 February 2006, paras. 118-154.
[56] MOYSE (fn. 52), at 60.
[57] See above II. 2.2. fn. 16.
[58] See above fn. 19.

agreed standards and practices to enhance security"[59], the proposal aims at laying out measures for effective international co-operation in dealing with cybercrime and terrorism. Illegal conduct includes the use of a cyber system as a material factor in committing a terrorist act[60]. Accordingly, an international consensus on the prohibition of any activity contributing to carrying out of terrorist acts is mirrored in the proposal[61].

50 ***2.3 Control measures as information channeling mechanisms***

Technical barriers to the dissemination of content in the Internet must keep in mind that certain institutions may disseminate the same information as terrorists, but in a legal way. An example thereof is information about how to build a bomb, which is considered illegal if used for terrorist purposes, but would be legal if disseminated by a chemistry physics online textbook[62]. A similar example from the past is the prohibition of the term "breast" in the Internet. While this prohibition was intended to serve for the protection of children from sex issues, all information related to breast cancer was also affected, even though this information is valuable to the public.

S. 66

51 As experience has shown, technological experts are capable to develop methods allowing to encounter such kind of situations. Possible approaches would be to install passwords, allowing only persons legally involved in the distribution of such information to have access.

52 Another approach would be to link searched keywords with other terms that are used only in the dissemination of information within the legal frame (e.g. link the word "breast" with the word "cancer"). If terms appear in this combination, the respective information does not have to be removed from the Internet. Respective technologies would observe the fact that only the use of the Internet for terrorist means violates the *ordre public*, not, however, the information itself.

53 ***2.4 Avoidance of terrorism as part of the ordre public***

Fighting terrorism as part of the *ordre public* is subject to change over time and measures to confront the problem have to be adapted correspondingly. While, for example, terrorism was understood rather in a national than in an international context a few decades ago, today, terrorism is understood primarily as an international phenomenon.

54 As *ordre public* represents fundamental values shared globally, an international court composed of members from all regions of the world is in the best position to assess whether a particular information has to be considered illegal, and determine what consequences this fact would have over time. The interests of all people have to be represented, which is unlikely to be realized in a national court. In particular, recent experiences after 9/11 show that the handling of terrorist acts as well as all acts related thereto, including the question of liability, should be considered by an international court. Unlike national courts, which may be inclined to seek revenge (communications according to which President Bush allegedly told to CIA to kill Osama Bin Laden point in that direction), international tribunals are composed of independent emotionally unattached judges[63]. A further possibility could consist in an extension of the catalogue of crimes conferring jurisdiction to the ICC[64].

55 In general, obligations under international law only bind the subjects of international

[59] Preamble of the Proposal for an International Convention on Cyber Crime and Terrorism.
[60] Art. 3 of the Proposal for an International Convention on Cyber Crime and Terrorism.
[61] See also ABRAHAM D. SOFAER/SEYMOUR E. GOODMAN/MARIANO-FLORENTINO CUÉLLAR/EKATERINA A. DROZDOVA/DAVID D. ELLIOT/GREGORY D. GROVE/STEPHEN J. LUKASIK/TONYA L. PUTNAM/GEORGE D. WILSON, A Proposal for an International Convention on Cyber Crime and Terrorism, available at <http://www.iwar.org.uk/law/resources/cybercrime/stanford/cisac-draft.htm>.
[62] COUNCIL OF EUROPE (fn. 4), at 64.
[63] HEINTZE (fn. 10), at 47; see also MARTIN (fn. 9), at 226-260.
[64] HELEN KELLER/DANIELA THURNHERR, Taking International Law Seriously, Berne 2005.

law. Accordingly, *ordre public* as a source of international law binds states in particular. However, already five decades ago, the perception that fundamental rights can also bind private parties evolved in Germany. According to this theory, developed in the context of the application of fundamental rights values in cases in which two private parties were involved, the rights of the German Grundgesetz (Basic Law) are not only defensive rights directed against the state, but they constitute an objective order of values ("eine objektive Werteordnung") which permeates the whole German legal system. The *Lüth-Decision*[65] of the Federal Constitutional Court led to a consistent jurisprudence in support of this theory on the so-called "mittelbare Drittwirkung", pursuant to which the values and principles surrounding constitutional fundamental rights are to be considered by the courts when deciding private law cases. The German approach on "Drittwirkung" has influenced legal orders outside Germany, especially the member states of the European Convention on Human Rights (ECHR)[66] and Japan. This perception of basic rights makes rights and freedoms become basic standards of social life, comprising a major part of the relationships between private individuals. However, the actual extent of this conception remains controversial[67].

S. 67

56 Most human rights, including the right to life, take effect on the horizontal level and require states to take measures to prevent violations of these rights by private persons, in particular by adopting laws and establishing effective implementation and enforcement procedures, i.e. they produce effect on the horizontal level between private parties[68]. Other than the concept of "Drittwirkung", the horizontal effect is not limited to the repercussions that basic human rights have on relationships under private law, but also include states' obligations to take further measures in order to protect human rights against interference by private parties[69].

57 However, the respective concept does not allow the imposition of direct obligations on private parties, rather it opts for an obligation of states through their public authorities in order to protect human rights from violations committed by non-state actors[70]. The introduction of specific regulation at the national level is necessary in order to directly oblige non-state actors to adhere to fundamental human rights; respective provisions can be found in several national orders[71]. Considering the importance of the prohibition of terrorism, a generally applicable, mandatory obligation of private parties to refrain from contributions to terrorist acts, and the possibility to hold these actors liable if they do not comply with this obligation appears to be worth to be established.

58 ## IV. Implementation

1. Technological measures

While the concept of *ordre public* is theoretical, measures have to be found to translate this concept into the practical world. Concerning the Internet framework, in particular technical measures may be adequate to decrease terrorist activities, thereby contributing to the implementation of the *ordre public*. Such technical measures are to be implemented by the Internet providers based on the concept of horizontal effects of human rights.

59 #### *1.1 Content monitoring*

[65] Deutsches Bundesverfassungsgericht (German Federal Constitutional Court), 15 January 1958.
[66] Council of Europe, European Convention on Human Rights, done at Rome on 4 November 1950.
[67] See ANNE CHEUNG/ROLF H. WEBER, Internet Governance and the Responsibility of Internet Service Providers, Wisconsin International Law Journal, Vol. 26, 2008, at 438-441, with further references.
[68] MANFRED NOWAK, UN Covenant on Civil and Political Rights: CCPR Commentary, 2nd ed. Kehl am Rhein 2005, at Introduction, para. 4; KAUFMANN (fn. 49), at 42-43.
[69] NOWAK (fn. 68), at § 2, para. 20; for the obligation of states to protect the security and physical integrity of their citizens in particular see NOWAK (fn. 68), at § 9, para. 7.
[70] CHEUNG/WEBER (fn. 67), at 439.
[71] For examples see CHEUNG/WEBER (fn. 67), at 437-449.

Different kinds of software-based architectural solutions could contribute to the elimination of illegal content on the Internet. In particular the use of filtering machines[72] being able to block certain sites that should not be accessible by the public can be very effective. However, experience has shown that this approach has not been widely used, and that technological solutions are at best a narrow and short-term remedy.

S. 68

60 (1) The mixture of languages makes it difficult to determine the content of each message. Furthermore, the use of passwords also complicates the job of monitors of Internet content. Nevertheless, using modern technology, inspectors should be able to access all information displayed online[73]. In order to pay respect to individuals' privacy, examining the content of private messages should only be admissible if a court allows it. Known terrorists are the prime candidates for a respective measure. Identifying messages between them is indispensable to protect human rights and thereby realizing the obligations under the prohibition of terrorism as part of the *ordre public*, obliging all members of society to contribute to that goal.

61 (2) Another measure would be to install rating systems built into the Internet browser software as a "content advisor", which can contain options for restricting access to illegal sites. Furthermore, it is possible to link the software to a rating platform, such as the Platform for Internet Content Selection Rules (PICS). PICS was developed in 1995 by the World Wide Web Consortium and enabled Web publishers to mark their websites with computer-readable metatags rating the content of the respective website. The idea of this program was to restrict access to certain Internet content, without having to censor the respective information altogether[74]. However, critics argued that this program could also be used by, in particular, repressive, governments to filter content automatically without input from the end user[75]. Nevertheless, the program is still in use, although it has been replaced to a large degree by the Resource Description Framework (RDF), which also rates Internet content[76]. If recruitment of terrorists, financing of terrorist actions, search of information on how to build bombing devices etc. are no longer possible in the online world, the address range of terrorists and their possibilities concerning terrorist activities will be highly delimited. As the carrying-out of terrorist acts becomes difficult, their number will decrease. This fact reflects the effectiveness of Internet content monitoring technologies, contributing to the respect of the *ordre public*[77].

62 Experience has shown that systems of Internet blocks and filters are difficult to handle. Technological innovation usually allows existing hurdles to be overcome in a relatively short time. Computer hackers around the world use their knowledge to find alternative technical solutions to get results that should not be achieved by individuals. A conse-

[72] For the filtering of data carried on the Internet see LESSIG (fn. 29), at 157.
[73] An example for an according mechanism able to decrypt passwords is the code-named "Magic Lantern" used by the FBI. Magic Lantern is a program which is sent to the suspect's computer, installs itself and then records every keystroke typed; these are analyzed by the FBI to find passwords enabling the FBI to access the suspect's e-mail, documents and computers contacted by the suspect; WEIMANN (fn. 1), at 188; FLORIAN RÖTZER, FBI bestätigt Entwicklung des Schnüffelprogramms Magic Lantern, available at < http://www.heise.de/tp/r4/artikel/11/11333/1.html>.
[74] WEBER (fn. 1), at 202; BIEGEL (fn. 27), at 201-202; LESSIG (fn. 30); see also <http://www.w3.org/PICS/>.
[75] JEREMY MALCOLM, Multi-Stakeholder Governance, Perth 2008, at 68.
[76] MALCOLM (fn. 75), at 81; for RDF in general see <http://www.w3.org/RDF/ >.
[77] The use of Carnivore, officially named DCS 1000, is another mechanism to monitor Internet content used by the FBI. Carnivore is comparable to a telephone wiretap, but applied to the Internet. It examines packets of information exchanged and records those that relate to suspicious issues. It is in particular used to intercept online communication (such as e-mail) passing through the Internet. Carnivore itself remains passive and does not change contents or messages. However, it scans millions of e-mails per seconds. The main concern of Carnivore is that it gives the FBI access to the traffic of all users of a given Internet service provider, not only those identified by a court, which infringes the right to privacy of many users; WEIMANN (fn. 1), at 184-187; see also <http://usgovinfo.about.com/library/weekly/aa080601a.htm>; <http://www.cotse.net/privacy/carnivore.htm; <http://epic.org/privacy/carnivore/>.

quence of this situation is the need to quickly change software filter programs[78]. The fact that systems have to be adapted continuously in order to pay respect to technological progress is also advantageous with view to the *ordre public*, as the *ordre public* can be subject of change according to the world's population's perception, too. By constant work on technological measures, the existence and definition of the prohibition of terrorism has to be kept in mind and eventual changes will most probably be recognized within a short period of time.

S. 69

63 (3) In 2000, the United States proposed the establishment of an international cyberpolice to fight cybercrime. This cyberpolice would be worldwide in coverage and participation and allow for rapid investigations over global communication networks. However, the project was not realized because the European Union opposed to the establishment of such a body arguing that there were privacy implications and differences among states in the definition of cybercrime[79].

64 (4) Capturing traffic over the Internet is called "sniffing"; the software searching the traffic and grabbing the searched information being the "sniffer". Technologically, sniffers use computers which are constantly communicating with other computers, most often using a local area network. This network uses filters to block or not to block users from getting the respective information. If the network is not "switched", the information is broadcast to every computer. The sniffer program tells a computer to monitor the traffic of information between all computers, peels away the layers of encapsulation and decodes the relevant information, including the identities of the source and of the target computer, and every piece of information exchanged between these two computers[80].

65 (5) In addition to the elimination of illegal content, ongoing monitoring of Internet content is also necessary to effectively fight against cyberterrorism. Possible approaches are to monitor the Internet by eavesdropping on e-mail and phone calls. These measures allow to track terrorists and criminals based on their online moves, such as using a credit card, sending an e-mail message, booking a flight, or paying a toll as respective activities leave an electronic trail[81]. Suspicious messages of potential terrorists have to be searched and identified, as well as distinguished from the everyday electronic traffic of millions of Internet users[82]. Messages exchanged between these persons are of high value to bodies fighting terrorism, as they give information about the terrorists' locations, planned attacks, etc. Only with this information available, the responsible bodies will be able to prevent violations of human rights and thereby contribute to compliance with the *ordre public*.

66 ***1.2 Storing of Internet content***

In March 2006, the European Parliament and the Council of the European Union enacted the Data Retention Directive[83], requiring all providers of electronic communications services and networks to keep traffic data related to phone calls and e-mails for a period of six months to two years[84]. Traffic data is defined to include the information necessary to identify the originator and the recipient of phone calls and e-mails, together with information on the time, date, and duration of these phone calls and emails[85]. Such data must be made available to the law enforcers at the national level, as well as to law enforcers in other member states[86]. In turn, state authorities are re-

[78] WEBER (fn. 1), at 194.
[79] WEIMANN (fn. 1), at 238.
[80] WEIMANN (fn. 1), at 183-184.
[81] WEIMANN (fn. 1), at 182.
[82] WEIMANN (fn. 1), at 183.
[83] Council Directive 2006/24/EC, 2006 O.J. (L 105) 54-58.
[84] Art. 6 Data Retention Directive.
[85] Art. 5 Data Retention Directive.
[86] Art. 4 Data Retention Directive.

quired to comply with the procedural standard of necessity and proportionality in their legal implementation, set out by Article 8[87]. Member states are expected to transpose the requirements of the Directive into national laws until March 2009[88]. The 2006 enactment can be seen as an attempt to strike a reasonable balance between law enforcement, combating of terrorist activities, and crime investigation on the one hand, and the protection of privacy on the other[89].

S. 70

67 Despite the advantages of modern technological measures to fight against illegal content on the Internet, the use of advanced techniques to monitor, search, track, and analyze Internet content, these techniques also hand participating governments, especially authoritarian governments and agencies with little public accountability, tools with which to violate civil liberties domestically and abroad[90].

68 For similar reasons, ZITTRAIN also considers the storing of Internet traffic an "awful idea": If the examination of Internet communications becomes routine rather than a reaction to a specific suspicion, the right to privacy of individual persons is violated. As according monitoring is unnoticeable to Internet users, data collected would remain in the hands of the collecting body, without users ever knowing it[91]. Different interests have to be balanced in every case of taking a specific measure to delimit Internet content; information put online must not be censored on a general basis. Furthermore, if information is denied access or removed, this measure must be declared to the user wanting to put the respective content on the Internet.

69 The prohibition of terrorism being part of the *ordre public* requires the responsible authorities to take all measures necessary for the attainment of this goal. This may include the storing of Internet traffic. However, with view to the speed of exchange of information and the mobility of terrorists, it is debatable whether the storing of data is absolutely necessary to eliminate terrorism as a phenomenon. Flows of information have to be detected and eliminated promptly in order to prevent terrorist attacks; the storing of data by itself does not contribute to the elimination of terrorism.

70 In order to address this problem of potential abuse, a body responsible for monitoring the activities of individual governments needs to be established, preferably at the international level. A possible approach to ensure that the fight against illegal content on the Internet is not misused would be to oblige governments to inform the respective body of the action they intend to take concerning this issue. The body then has to assess the admissibility of the respective measure and give its approval to the concerned government.

71 In general, better information about terrorists' uses of the Internet in order to monitor their activities is necessary to develop the technical infrastructure to prevent the dissemination of illegal content on the Internet.

72 **2. Liability of Internet providers**

Internet providers have a controlling position in respect of Internet content and should therefore carry a corresponding responsibility; controlling Internet content is not only a power, but also an obligation. However, most general criminal law rules of participation are insufficient to address the problem of dissemination of illegal terrorist content on the Internet. Special legislation is required to prevent the respective information and to

[87] Art. 8 Data Retention Directive.
[88] Art. 15 Data Retention Directive.
[89] CHEUNG/WEBER (fn. 67), at 473; see generally FRANCESCA BIGNAMI, Privacy and Law Enforcement in the European Union: The Data Retention Directive, Chinese Journal of International Law, Vol. 8, 2007, 233-255.
[90] WEIMANN (fn. 1), at 58.
[91] JONATHAN ZITTRAIN, Beware the Cyber Cops, Forbes, Vol. 170 (8 July 2002), at 62.

enforce provisions by defining responsibility[92].

S. 71

73 Internet providers are not directly bound by human rights. However, horizontal effects and the theory of "Drittwirkung" of the right to life in terms of a state obligation are generally acknowledged. Horizontal effects of human rights do not impose direct obligations on Internet providers[93]. Nevertheless, the question of liability of Internet providers if illegal, terrorism-related content is disseminated is addressed in the following.

74 Internet providers can filter or censor information[94]. This ability should not only be a power of Internet providers, but also an obligation to prevent the dissemination of illegal content. In Europe, a consensus is emerging that Internet providers should be held responsible for controlling content disseminated on the Internet. The E-Commerce-Directive of June 2000[95] distinguishes between providers "providing access to the Internet" and providers offering other services, in particular "providing hosting content", produced by themselves or by other users.

75 On the basis of this distinction, different degrees of liability can be established, according to the function of the provider and its direct contact to the content. The E-Commerce-Directive addresses the problem of holding providers liable for the dissemination of illegal information. In cases of involving the "mere conduit" of data, access providers are exempted from liability; providers are not obliged to monitor the dissemination of information (Art. 15). Providers of hosting content are only liable in cases involving the storing of data if they have actual knowledge of illegal activity or information (Art. 14). Meanwhile, it is generally acknowledged that providers putting a special emphasis on their editorial role should be fully liable if illegal content is disseminated; if the content originates from elsewhere, providers should be liable to the extent the are informed of the illegality of the content and it was feasible for the to identify and technically control the material in order to remove it from online circulation[96]. However, if operators only provide access to the Internet, without having any influence on its content, liability should only be established if they are themselves the content-providers or if they had been informed of the illegal content and did not take the steps necessary to remove it from a service offered.

76 Thus, as a rule, Internet providers should be held liable if they themselves contributed to the dissemination of illegal content or were informed and failed to take the necessary steps to prevent it[97]. A broad responsibility of Internet providers is justifiable considering the enormous negative effect the dissemination of illegal content may have. This approach does not burden Internet providers with insurmountable difficulties in complying with the respective provisions, either. Appropriate law-enforcement or self-regulatory bodies or will have to be appointed to enforce liability regulations[98].

77 Establishing liability for Internet providers is not only ensuring a free exchange of information and legal certainty for Internet providers, but also ensures prosecution of past crimes and prevents the dissemination of illegal content in the future. It furthermore provides the basis for "notice and takedown procedures"[99], contributing to the elimination of illegal content on the Internet. Hotlines collecting tips from users concerning illegal information can induce Internet providers to take down illegal content so that the respective information is no longer accessible to the public; the police can

[92] COUNCIL OF EUROPE (fn. 4), at 72.
[93] See above III. 2.4, fn. 65-70.
[94] CHEUNG/WEBER (fn. 67), at 408-411.
[95] Council Directive 2000/31/EC, 2000 O.J. (L 178), 1-16.
[96] See also COUNCIL OF EUROPE (fn. 4), at 72-73; SIEBER (fn. 36), at 370-374.
[97] GREWLICH (fn. 14), at 275-276.
[98] GREWLICH (fn. 14), at 276.
[99] COUNCIL OF EUROPE (fn. 4), at 73.

even force them to do so[100].

S. 72

78 However, the identification of providers can be difficult. Therefore, rules have to be established obliging providers to keep a log of usages for a certain period. This obligation, though, asks for another balancing of interests between the will to prevent the dissemination of illegal terrorist information on the Internet and the privacy of Internet users wanting to disseminate content through providers[101].

79 Tendencies to hold non-state actors liable under international law can be discerned. Obligations concerning the conduct of private actors are displayed in many (non-binding) international codes. These codes may influence the field of activity of Internet providers. Furthermore, Internet providers should become active themselves by applying self-regulative codes of conduct[102].

80 **3. Soft sanctions for countries not co-operating**

Terrorism in general is prohibited by the international *ordre public*. The obligation to ensure that the prohibition of terrorism is realized addresses all states; governments have to guarantee that the respective prohibition is effectively implemented within their territories. This fact requires states to co-operate because most terrorists nowadays act internationally and the Internet has a global dimension. Disseminating illegal terrorist content contributes to terrorist acts, which are a threat to peace and justify sanctions for countries which do not co-operate in the effort to eliminate such contributions. Soft law, and in particular soft sanctions, is not a poor relation to hard law and may be the best form of governance for international co-operation. However, before any sanctions are taken against a state not complying with its obligations, the respective state should be formally warned.

81 Sanctions are considered "soft" if they do not use force. However, they can consist in complete or partial interruption of economic relations and of rail, sea, air, postal, telegraphic, radio, or other means of communication as well as in the severance of diplomatic relations. Such sanctions are contained in Art. 41 of the Charter of the UN[103]. Further soft sanctions would be to impose a fine on the state not complying with its obligation to co-operate or the termination of humanitarian assistance. States are free in their choice of soft sanctions, which do not have to be proportionate or previously announced to the concerned state[104]. Sanctions must be supervised during their being in force. If the state complies with its obligation to ensure that human rights are not violated and takes respective measures, the sanctions have to be suspended.

82 The issue of the efficacy of sanctions is still controversially discussed. However, the damage that, in particular economic, sanctions may do to the civil society of a state, especially if the state does not operate in good faith, may be devastating. Therefore, sanctions should only be taken as an *ultima ratio*, and it should be made sure they do not affect the population, but rather the decision-making authorities[105].

S. 73

83 **V. Conclusions**

The abuse of the Internet is a global threat. Therefore, the dissemination of illegal content on the Internet, including terrorist information, has to be tackled. Existing meas-

[100] COUNCIL OF EUROPE (fn. 4), at 73; SIEBER (fn. 36), at 367.
[101] GREWLICH (fn. 14), at 291.
[102] CHEUNG/WEBER (fn. 67), at 454.
[103] For powers of the Security Council under Art. 41 UN Charter see ERIKA DE WET, The Chapter VII Powers of the United Nations Security Council, Portland 2004, at 178-255; see also MARTIN (fn. 9), at 500-518.
[104] IPSEN (fn. 21), at § 59 N 44.
[105] See also CHRISTINE KAUFMANN, Menschenrechtspolitik und freier Handel – ein Widerspruch?, in: Neue Zürcher Zeitung vom 9. September 2006, at 75; MARTIN (fn. 9), at 519-525.

ures are not sufficient to satisfactorily solve this problem. New mechanisms need to be established, preferably at the international level; the Internet as a global framework and the worldwide movement of terrorists ask for an international regulation. States can either co-operate directly, or co-operation can be institutionalized and take the form of an international body which represents a common understanding of all states.

84 Many international Conventions on terrorism in general are already in existence. However, provisions concerning international co-operation need to be concretized and measures have to be found to effectively implement and enforce them. Furthermore, the problem of terrorist use of the Internet needs to be more specifically addressed in international agreements.

85 The fact that terrorism merits to be prohibited is commonly acknowledged and constitutes part of the international *ordre public*. Terrorist acts violate human rights, in particular the right to life as one of the most fundamental human rights. The goals of terrorists do not justify violations of these rights. However, the outcome of the balancing between security interests and, in particular, freedom of speech, is controversially discussed.

86 If the security interests outweigh the individual's rights to freedom of speech or open communication in a particular case, the illegal information has to be removed from the Internet. However, not only repressive, but also preventive actions need to be taken. Preventive efforts can consist in the introduction of technological barriers, the threat for Internet providers of being held liable or the threat for nation states of being sanctioned for not complying with their obligations.

Zitierempfehlung: Rolf H. Weber/Romana Weber, HFR 2009, S. 52 ff.