Articles

Principles of International Internet Law

By Robert Uerpmann-Wittzack[*]

Abstract

Legal principles are an essential element of jurisprudence. They help to systemize, to comprehend and to further develop a legal order. Although International Internet Law is quite a new legal subject, some principles begin to evolve. The article addresses five emerging core principles of International Internet Law: (1) The principle of internet freedom, (2) the principle of privacy, (3) a modified principle of territorial jurisdiction adapted to cyberspace, (4) the principle of interstate cooperation, and (5) the principle of multi-stakeholder cooperation.

A. Introduction

International Internet Law (IIL) is a fairly new subject. Although the origins of the internet date back to the 1960s,[1] its political and economic importance only became visible at the beginning of the 1990s. By that time, legal scholars had become interested in questions of internet governance. IIL is the common denominator for all rules of public international law pertaining to the functioning and use of the internet. Furthermore, IIL is a cross-sectional matter which comprises, *inter alia*, questions of human rights, and of international economic and institutional law.[2] Some problems have already given rise to intensive legal debate on this subject. The most prominent example is the administration of the Internet Domain Name System (DNS) by the Internet Corporation for Assigned Names and Numbers (ICANN).[3] The debate on domestic jurisdiction over internet content

[*] Email: Robert.Uerpmann-Wittzack@jura.uni-regensburg.de

[1] See ANDREW D. MURRAY, THE REGULATION OF CYBERSPACE 60-69 (2007).

[2] See Robert Uerpmann-Wittzack, *Internetvölkerrecht*, 47 ARCHIV DES VÖLKERRECHTS (AVR) 261, 263-274 (2009).

[3] See *e.g.* Hans-Georg Dederer, *ICANN und die Dominanz der USA*, 47 AVR 367 (2009); Wolfgang Kleinwächter, *From Self-Governance to Public-Private Partnership: The Changing Role of Governments in the Management of the Internet's Core Resources*, 36 LOYOLA OF LOS ANGELES LAW REVIEW 1103 (2003); *Id., Beyond ICANN vs. ITU: Will WSIS Open New Territory for Internet Governance?*, in INTERNET GOVERNANCE: A GRAND COLLABORATION 31, 36 (Don McLean ed., 2004); Robert Uerpmann-Wittzack, *Multilevel Internet Governance Involving the European Union, Nation States and NGOs*, in MULTILEVEL REGULATION AND THE EU 145 (Andreas Follesdal, Ramses A. Wessel & Jan Wouters eds., 2008).

located on servers abroad is no less controversial.[4] E-commerce is an important topic for the World Trade Organization (WTO)[5] and for other international organizations.[6] As the internet penetrates all areas of human life, IIL virtually touches upon all fields of international law. Debates on cyber war, for instance, involve questions of *ius ad bellum*[7] and international humanitarian law.[8] Due to its cross-sectional approach, IIL might appear heterogeneous or even incoherent. However, some underlying principles are noticeable. This article deals with the emerging principles of IIL.

Legal principles have at least two different functions.[9] First, they help to systemize and, by that, to explain a set of legal rules. By virtue of this function, an incoherent mass of legal rules turns into a legal order. This does not necessarily imply an idea of completeness. The international legal order is still fragmentary because international law is only needed where existing problems cannot be solved satisfactorily by domestic law. Principles may be laid down in legal texts like Article 2 United Nations Charter or they may be recognized by states in international declarations. In the absence of such recognition, legal doctrine may propose legal principles which seem appropriate to systemize a set of legal rules.

Secondly, principles are an element of legal reasoning.[10] They help to construe given rules of international law and to elucidate their object and purpose. Thus, international treaties may be interpreted in the light of their underlying legal principles. Legal principles may also influence the evolution of international customary law. While it is true that international custom essentially relies on state practice, state actors may recur to legal principles in

---

[4] See UTA KOHL, JURISDICTION AND THE INTERNET (2007).

[5] See the WTO, Work Programme on Electronic Commerce, WTO Doc. WT/L/274 of 30 September 1998.

[6] See Christian Tietje & Karsten Nowrot, *Das Internet im Fokus des transnationalen Wirtschaftsrechts: Normative Ordnungsstrukturen für den E-Commerce*, 47 AVR 328 (2009).

[7] See Christopher C. Joyner & Catherine Lotrionte, *Information Warfare as International Coercion: Elements of a Legal Framework*, 12 EUROPEAN JOURNAL OF INTERNATIONAL LAW (EJIL) 825 (2001); Wolff Heintschel v. Heinegg, *Informationskrieg und Völkerrecht*, in BRÜCKEN BAUEN UND BEGEHEN: FESTSCHRIFT FÜR KNUT IPSEN 129 (Volker Epping, Horst Fischer & Wolff Heintschel v. Heinegg eds., 2000); Antonio Segura-Serrano, *Internet Regulation and the Role of International Law*, 10 MAX PLANCK YEARBOOK OF UNITED NATIONS LAW (MPYUNL) 191, 220-231 (2006).

[8] Michael N. Schmitt, *Wired Warfare: Computer Network Attack and jus in bello*, 84 INTERNATIONAL REVIEW OF THE RED CROSS 365 (2002); Jenny Döge, *Cyber Warfare: Challenges for the Applicability of the Traditional Laws of War Regime*, 48 AVR (2010; forthcoming).

[9] See Armin von Bogdandy, *Founding Principles*, in PRINCIPLES OF EUROPEAN CONSTITUTIONAL LAW, 11, 14-18 (Armin von Bogdandy & Jürgen Bast eds., 2nd ed., 2009), who discerns even three functions of legal principles; see also *Id., General Principles of International Public Authority: Sketching a Research Field*, 9 GLJ 1909, 1910-1914 (2008); András Jakab, *Re-Defining Principles as "Important Rules": A Critique of Robert Alexy*, in ON THE NATURE OF LEGAL PRINCIPLES 145, 155-159 (Martin Borowski ed., 2010).

[10] PIERRE-MARIE DUPUY, DROIT INTERNATIONAL PUBLIC (9th ed. 2008), para. 334.

order to justify a corresponding rule of international custom. Frequently, international courts and scholars also advance legal principles within a reasoning based on international custom. The well established rule that state jurisdiction requires a genuine link even refers directly to ideas of reasonableness[11] and to certain legal principles.

These legal principles are different from the concept of general principles of law, which is laid down in Article 38(1)(c) of the Statute of the International Court of Justice (ICJ). The latter being derived from domestic law,[12] and are used to fill gaps in international law which occur *e.g.* with regard to the judicial process.[13] By contrast, this article covers legal principles originating from international law. Some of these principles may have parallels in domestic legal orders, whereas others refer exclusively to the international sphere. Unless these principles are laid down in international treaties or derive from customary law, they are close to the subsidiary sources of Article 38(1)(d) ICJ Statute. They are part of legal doctrine. When applying sources of international law, courts and legal scholars may argue in terms of legal principles.

Although IIL is still a young field of legal scholarship, some principles are evolving. This article addresses five core principles: (1) The principle of internet freedom, (2) the principle of privacy, (3) a modified principle of territorial jurisdiction adapted to cyberspace, (4) the principle of interstate cooperation, and (5) the principle of multi-stakeholder cooperation. The concluding section shall analyze how these principles regulate the interrelationship between different actors with regard to the internet.

B. The Principle of Internet Freedom

The freedom of internet communication, which is firmly rooted in international human rights law, is at the core of internet freedom. Yet, it is questionable whether internet freedom also comprises commercial internet freedoms. This section shall address (I) freedom of internet communication, and (II) freedom of internet business.

---

[11] See Stefanie Schmahl, *Zwischenstaatliche Kompetenzabgrenzung im Cyberspace*, 47 AVR 284, 313 (2009).

[12] See IAN BROWNLIE, PRINCIPLES OF PUBLIC INTERNATIONAL LAW 16 (7th ed., 2008); DUPUY (note 10), para. 331.

[13] ANTONIO CASSESE, INTERNATIONAL LAW 193-194 (2nd ed., 2005).

I. Freedom of Internet Communication

Freedom of expression is the essential freedom of the internet. Article 19(2) of the Covenant on Civil and Political Rights (CCPR)[14] guarantees this freedom on a universal level. In Europe, a corresponding right is enshrined in Article 10 of the European Convention on Human Rights (ECHR).[15] Article 19(2) CCPR expressly refers to expression "through any … media of his choice".[16] Although Article 10 ECHR is silent on this point, it is clear that the European Convention equally protects expression through the internet. Information and ideas expressed on a webpage fall within the scope of Article 10 ECHR.[17] In *Times Newspaper Ltd. v. United Kingdom*, the European Court of Human Rights recently found that internet archives fall within the scope of Article 10 ECHR.[18] As freedom of expression comprises freedom of information, it entitles not only content providers but also simple internet users.[19] Although neither Article 19 CCPR nor Article 10 ECHR mention freedom of the press, the European Court of Human Rights has emphasized the importance of the press for a democratic society and its role as public watchdog.[20] This is also true for the electronic press. In *Fatullayev v. Azerbaijan*, the European Court of Human Rights explicitly assimilated a popular internet forum to the printed media in terms of effect.[21] It is worth while noting that both texts guarantee freedom of expression "regardless of frontiers". This is particularly important for the internet, which defies national borders.[22]

Unlike rules, principles do not require strict observance. Due to their broad scope, they easily collide with other principles or interests. In this case, the principle has to be realized as far as this is possible under the given legal and factual circumstances.[23] Regarding

---

[14] UNTS, vol. 999, 171, 178.

[15] Council of Europe Treaty Series No. 5, available at: http://conventions.coe.int/.

[16] UNTS, vol. 999, 171, 178.

[17] Eur. Court H.R., *Perrin v. United Kingdom*, Judgment of 18 October 2005, Reports of Judgments and Decisions 2005-XI.

[18] Eur. Court H.R., *Times Newspapers Ltd v. United Kingdom (nos. 1 and 2)*, Judgment of 10 March 2009, Application 3002/03 and 23676/03, para. 27.

[19] *Id.*

[20] Eur. Court H.R., *Observer and Guardian v. United Kingdom*, Judgment of 26 November 1991, Series A, No. 216, para. 59; *Times Newspapers Ltd v. United Kingdom* (note 18), para. 40.

[21] Eur. Court H.R., *Fatullayev v. Azerbaijan*, Judgment of 22 April 2010, Application 40984/07, para. 95.

[22] Nicola Wenzel, *Opinion and Expression, Freedom of, International Protection*, in MAX PLANCK ENCYCLOPEDIA OF PUBLIC INTERNATIONAL LAW (MPEPIL, Rüdiger Wolfrum ed., 2009), para. 14, available at http://www.mpepil.com/.

[23] See ROBERT ALEXY, A THEORY OF CONSTITUTIONAL RIGHTS 47-48 (2002): principles as optimization requirements; see also Martin Borowski, *The Structure of Formal Principles – Robert Alexy's "Law of Combination"*, in ON THE NATURE OF LEGAL PRINCIPLES (note 9), 19, 20-22.

internet freedom, the European Court of Human Rights admitted the importance of state control in *Megadat.com v. Moldova*.[24] Articles 19(3) CCPR and 10(2) ECHR reflect this structure. They contain lists of legitimate aims which may justify an interference. These aims include principles and interests such as the rights of others, national security, public order and morals. In case of conflict, a fair balance must be struck between the competing interests.[25] This is realized by the necessity test laid down in Articles 19(3) CCPR, 10(2) ECHR and requires the interference to be proportionate to the legitimate aim pursued.[26]

II. Freedom of Internet Business

Internet freedom is more than freedom of expression. The internet as a means of communication depends on the functioning of its infrastructure. Therefore, internet freedom should comprise the freedom of internet providers, at which point commercial freedoms come into play. International human rights law hardly grants commercial freedoms. Rather, these are a concern of World Trade Law. This section shall look at (1) human rights law, and (2) World Trade Law.

1. Human Rights Law

In contrast to national constitutions, international law neither guarantees the freedom to choose an occupation nor the freedom to conduct a business.[27] However, internet providers enjoy freedom of expression even if their activities are of a commercial nature, and may therefore invoke freedom of expression against interferences with regard to content. For instance, in *Times Newspaper Ltd.*, the European Court of Human Rights concluded that ceaseless liability for defamatory article content in an internet archive interfered with the company's freedom of expression.[28] Such interference is not illegal *per se*, but it requires a special justification.

---

[24] Eur. Court H.R., *Megadat.com SRL v. Moldova*, Judgment of 8 April 2008, Application 21151/04, para. 68.

[25] Eur. Court H.R., *Von Hannover v. Germany*, Judgment of 24 June 2004, Reports of Judgments and Decisions 2004-VI, paras. 57-58.

[26] See Dirk Ehlers, *General Principles*, in EUROPEAN FUNDAMENTAL RIGHTS AND FREEDOMS 25, 53 (Dirk Ehlers ed., 2007).

[27] But see Articles 15, 16 of the Charter of Human Rights of the European Union, O.J. 2007 C 303/1; moreover, Article 6 of the International Covenant on Economic, Social and Cultural Rights (GA Res. 2200 [XXI] of 16 December 1966) as well as Article 1 of the European Social Charter of 18 October 1961 (Council of Europe Treaty Series No. 35) guarantee the social right to work.

[28] Eur. Court H.R., *Times Newspapers Ltd* (note 18), para. 37 and *passim*.

Although the ECHR does not protect commercial activity as such, an internet provider may in extreme cases rely upon its right to property enshrined in Article 1 of the First Protocol to the ECHR. In *Megadat.com* the European Court of Human Rights held that a license for providing internet services was a possession within the meaning of Article 1 First Protocol, and that the termination of the license amounted to interference.[29] Registered domain names are another example of internet property rights protected by this article.[30] However, the ECHR remains far from granting an overall protection to internet service providers.

Protection is even weaker under the Covenant on Civil and Political Rights which contains no right to property. Companies do not even have standing before the Human Rights Committee under Articles 1 and 2 of the CCPR Optional Protocol No. 1 of 19 December 1966. While Article 34 ECHR permits complaints by non-governmental organizations, *i.e.* legal persons, the CCPR Optional Protocol restricts the right of standing to individuals.

2. World Trade Law

Freedom of transnational internet commerce might find a basis in World Trade Law. By prohibiting quantitative restrictions on import and export, Article XI General Agreement on Tariffs on Trade (GATT)[31] grants free market access. As far as trade in services is concerned, Article XVI General Agreement on Trade in Services (GATS)[32] provides market access as a specific commitment. Trade in internet hardware like servers and personal computers falls within the ambit of GATT.[33] By contrast, internet economy does not deal with the exchange of goods, *i.e.* physical products, but consists of trade in services, which is governed instead by GATS.

It is not easy to derive a principle of market access from GATS. Article XVI of GATS does not grant market access automatically. Rather, market access depends on the decision of states to include certain categories of services into their lists of specific commitments under Article XX of GATS.[34] It is hardly possible to establish a principle of market access

[29] Eur. Court H.R., *Megadat.com SRL* (note 24), paras. 62-64.

[30] Eur. Court H.R., *Paeffgen GmbH v. Germany*, Judgment of 18 September 2007, Application 25379/04 et al., sub The Law 1.

[31] UNTS, vol. 55, 188, 224-228.

[32] UNTS, vol. 1869, 183, 197.

[33] See *e.g.* WTO Appellate Body, *EC – Computer Equipment*, Report of 5 June 1998, WT/DS62/AB/R; WTO Panel, *EC – IT Products*, Report of 16 August 2010, WT/DS375/R, WT/DS376/R & WT/DS377/R.

[34] UNTS, vol. 1969, 183, 199.

unless most countries have undergone corresponding specific commitments. Moreover, services are defined in a way that is technically neutral. For instance, market access for internet gambling services depends on whether a state has given a specific commitment for gambling and betting services.[35] Supplying online does not constitute a distinct category of services.[36] In the absence of an overall category of internet services, it is difficult to establish a principle of internet market access.

Another objection relates to the legal character of market access under GATT and GATS. Ernst-Ulrich Petersmann[37] is a strong proponent of a constitutional approach which qualifies GATT and GATS guarantees as individual rights. However, his position is contested.[38] For a debate on principles, the question may remain open. A principle of market access may also exist if it can only be invoked by states and not by individuals.

Like any principle, market access is not a strict obligation. It can collide with other principles, and a fair balance must be struck. This is laid down in the general exceptions clauses of Article XX of GATT and Article XIV of GATS. Both articles enumerate competing principles such as the protection of public morals and order.[39] Although the WTO Appellate Body[40] applies the necessity test in a different way than the European Court of Human Rights, both judicial bodies weigh and balance the restrictive effect of a measure against its benefit. Therefore, the WTO Appellate Body held in *US – Gambling* that the protection of morals could in principle justify a restriction of, and even a total ban on, the freedom of internet gambling and betting services.[41]

---

[35] WTO Appellate Body, *US – Gambling*, Report of 7 April 2005, WT/DS285/AB/R, paras. 158-213.

[36] See also WTO Panel, *China – Publications and Audiovisual Products*, Report of 12 August 2009, WT/DS/363/R, paras. 7.1209, 7.1220.

[37] Ernst-Ulrich Petersmann, *The WTO Constitution and Human Rights*, 19 JOURNAL OF INTERNATIONAL ECONOMIC LAW 19 (2000); *Id., Human Rights, Constitutionalism and the World Trade Organization*, 19 LEIDEN JOURNAL OF INTERNATIONAL LAW 633 (2006).

[38] MARKUS KRAJEWSKI, VERFASSUNGSPERSPEKTIVEN UND LEGITIMATION DES RECHTS DER WELTHANDELSORGANISATION (WTO) 188-193 (2001); Armin von Bogdandy, *Law and Politics in the WTO*, 5 MPYUNL 609, 655-657 (2001).

[39] See Article XX(a) GATT, Article XIV(a) GATS.

[40] WTO Appellate Body, *US – Gambling* (note 35), paras. 304-327; *China – Publications and Audiovisual Products*, Report of 21 December 2009, WT/DS/363/AB/R, paras. 237-249.

[41] WTO Appellate Body, *US – Gambling* (note 35), para. 373(D)(iv).

C. The Principle of Privacy

The principle of privacy is equally enshrined in international human rights law. Article 17 CCPR protects one's privacy, family, home, correspondence, honour and reputation. Article 8 ECHR addresses private and family life, home and correspondence. Both articles have a broad scope of application which has been specifically developed by the European Court of Human Rights. It may be taken for granted that emails are protected correspondence within the sense of these articles.[42] Other data which is transmitted by the internet or which is accessible through the internet belongs to a person's private life, unless it is destined for public access. In *Copland v. United Kingdom*, the European Court of Human Rights had no problem qualifying an employee's use of the internet as part of her private life and correspondence.[43] In consequence, state control over private internet use and content including emails amounts to an interference. The same is true for an obligation of internet providers to store internet data as laid down in Article 3 of the European Directive 2006/24/EC on the retention of data generated or processed in connection with the provision of publicly available electronic communications services.[44] Even a person who does not use the internet may be compromised by the internet publication of information relating to him or her. If public authorities publish such information, or if legislation imposes a duty to publish it, the state interferes with private life, as the European Court of Human Rights rightly stated in *Wypych v. Poland*.[45] Legality therefore depends on a special justification.

Internet privacy is not only threatened by public authorities but also by private persons and enterprises. Enterprises and social community platforms store large amounts of private data which may compromise and harm an individual if they are stolen or otherwise misused. Moreover, a person may be affected by the internet publication of information relating to him or her. Online ratings of professionals such as teachers and physicians illustrate this. In such cases, states are under a positive obligation to protect privacy. This obligation becomes particularly clear in CCPR Article 17(2), according to which everyone has the right to legal protection against interference with his or her privacy. Even though

---

[42] See Eur. Court H.R., *Liberty et al. v. United Kingdom*, Judgment of 1 July 2008, Application 58243/00, para. 52; *Kennedy v. the United Kingdom*, Judgment of 18 May 2010, Application 26839/05, para. 118, where the Court makes, however, no distinction between private life and correspondence.

[43] Eur. Court H.R., *Copland v. United Kingdom*, Judgment of 3 April 2007, Application 62617/00, paras. 41-42.

[44] EP and Council Directive 2006/24 of 15 March 2006, O.J. 2006 L 105/54.

[45] Eur. Court H.R., *Wypych v. Poland*, Judgment of 25 October 2005, Application 2428/05; see also *G. v. Finland*, Judgment of 27 January 2009, Application 33173/05, para. 52, with regard to the publication of a judgment on the internet, and Human Rights Committee, *Sayadi & Vinck v. Belgium*, Views of 29 December 2008, UN Doc. CCPR/C/94/D/1472/2006, para. 10.12, with regard to the publication of personal data on a UN sanctions list via the internet.

the ECHR does not contain a similar specification, the European Court of Human Rights has derived positive obligations from Article 8 ECHR.[46]

It would be wrong, however, to focus exclusively on privacy. In the cases at hand, protection of privacy comes into conflict with internet freedom. Here, two separate principles of IIL collide. Whereas freedom of expression may be restricted in favor of the rights of others and in particular the right to privacy, any restriction must be proportionate to the aim pursued. States have to strike a fair balance between privacy on the one hand and internet freedom on the other hand.[47] If an individual is seriously compromised, the state must even envisage criminal sanctions.[48] In *K. U. v. Finland*,[49] an unknown person had placed an announcement on an internet dating site in the name of a 12 year old boy. At that time, the service provider could not be compelled under Finnish law to reveal the identity of the person who had placed the advertisement. Any prosecution was therefore excluded. In the view of the European Court of Human Rights, Finland had failed to abide by its positive obligation to protect the private life of the boy.[50]

D. The Principle of Territorial Jurisdiction

The negative obligations arising out of human rights norms limit public authorities in their scope of action. They create and guarantee an area of individual freedom, which is protected against state intervention. Jurisdiction, by contrast, deals with the relationship between states. Under a regime of sovereign equality, as laid down in Article 2(1) United Nations Charter, the jurisdiction of one state finds its limits in the jurisdiction of others. In consequence, the exercise of jurisdiction requires a genuine link. A state may exercise territorial jurisdiction over its state territory and personal jurisdiction over its citizens.[51]

---

[46] Eur. Court H.R., *Marckx v. Belgium*, Judgment of 13 June 1979, Series A, No. 31, para. 31; *Airey v. Ireland*, Judgment of 9 October 1979, Series A, No. 32, para. 32; *X and Y v. the Netherlands*, Judgment of 26 March 1985, Series A, No. 91, para. 32; see also *Benediktsdóttir v. Iceland*, Judgment of 16 June 2009, Application 38079/06, sub The Law 3 I; Robert Uerpmann-Wittzack, Personal Rights and the Prohibition of Discrimination, in EUROPEAN FUNDAMENTAL RIGHTS AND FREEDOMS (note 26), 67, 76.

[47] See, mutatis mutandis, Eur. Court H.R., von Hannover (note 25), paras. 57-58, for a conflict between privacy and freedom of the press.

[48] Eur. Court H.R., *X and Y v. the Netherlands* (note 46), para. 27; *K. U. v. Finland*, Judgment of 2 December 2008, Application 2827/02, para. 43.

[49] *K. U. v. Finland* (note 48).

[50] *K. U. v. Finland* (note 48), paras. 40-50.

[51] Bernard H. Oxman, *Jurisdiction*, in MPEPIL (note 22, 2007), para. 11.

The principle of territorial jurisdiction is well established in public international law.[52] However, two modifications can be discerned with regard to Cyberspace. First, the effects doctrine giving jurisdiction over foreign acts provided that they produce effects within the own territory must be adapted to the ubiquitous nature of the internet. Second, jurisdiction expands to a state's country code Top Level Domain which becomes cyber territory. This section shall explore the qualified effects doctrine, and (II) the Country Code Top Level Domain as Cyberterritory.

I. A Qualified Effects Doctrine

Article 22 of the European Convention on Cybercrime (ECC) of 23 November 2001[53] confirms the traditional principle of territorial jurisdiction. According to Article 22(1)(a) ECC each contracting party establishes jurisdiction over offences committed on its territory. It is well established that an offence is committed at the place where the perpetrator acted.[54] If a person places harmful content, such as pornography on a web site, the state where the person has actually worked on the computer may intervene. Traditionally however, it is accepted that an offence is also committed on the territory where the effects of a criminal act occur.[55] This objective territorial principle comes close to the effects doctrine which is established in antitrust law.[56] The Council of Europe Committee of Ministers confirmed the effects doctrine in its comment on Article 22 ECC. According to the Committee, a state should not only "assert territorial jurisdiction if both the person attacking a computer system and the victim system were located within its territory", but also "where the computer system attacked is within its territory, even if the attacker is not."[57] In this case there would indeed be a genuine link between the attack and the state where the victim's system is located because the targeted computer system exists in that country. The situation is less clear when harmful content is published through the internet. A webpage is in principle accessible from any point of the world. Under a wide effects doctrine,

---

[52] See BROWNLIE (note 12), 299, 301; DUPUY (note 10), paras. 66-73.; Lotus, PCIJ 1927, Series A, No. 10, 1, 18; Eur. Court H.R. (Grand Chamber), *Banković and Others v. Belgium and 16 Other Contracting States* , Judgment of 12 December 2001, Reports of Judgments and Decisions 2001-XII, para. 59.

[53] European Treaty Series No. 185, available at: http://conventions.coe.int/.

[54] Oxman (note 51), para. 16.

[55] Lotus (note 52) 23; Vaughan Lowe & Christopher Staker, *Jurisdiction*, in INTERNATIONAL LAW 313, 321-322 (Malcom D. Evans ed., 3rd ed. 2010); Oxman (note 51), para. 23.

[56] See Joined Cases 89/85 et al., *Wood Pulp*, 1988 E.C.R. 5193, paras. 15-18; Eleanor M. Fox, *Modernization of Effects Doctrine: From Hands-Off to Hands-Linked*, 42 NEW YORK UNIVERSITY JOURNAL OF INTERNATIONAL LAW AND POLITICS 159,160, 167, 174 (2009).

[57] Council of Europe, Committee of Ministers, Convention on Cybercrime, Explanatory Report of 8 November 2001, para. 233, available at: http://conventions.coe.int/treaty/en/reports/html/185.htm.

jurisdiction would be established by the mere fact that a prosecutor views a webpage with harmful content from his or her office desk. In *Perrin*, British courts convicted a French national of publishing obscene material on a US website because a police officer had viewed it in a London police station.[58] In *Toeben*, German courts convicted an Australian national of Holocaust denial on an Australian website.[59] In *Yahoo*, the Tribunal de Grande Instance de Paris (Paris Regional Court) found that offering Nazi memorabilia on a US server violated French criminal law.[60] If no restriction was made, World Wide Web content would have to comply with the legal orders of more than 190 states. Due to the transnational character of the internet, the simple possibility to view a webpage in any country cannot be sufficient in order to establish a genuine link between the webpage and the prosecuting state.

This view is widely accepted by courts and scholars.[61] Therefore, different attempts have been made to restrict the effects doctrine in a way which takes the ubiquitous nature of cyberspace into account. US courts rely on a reasonable effects doctrine.[62] Although court practice throughout the world is not uniform, there is a strong tendency to use several criteria in order to determine whether a webpage has a sufficient link to a given country. These criteria include the language as well as the content or publicity[63] which refers to a specific country.[64] If web content is intended to be retrieved from a specific country, this country has a good claim to jurisdiction.[65] In *Toeben*, the Bundesgerichtshof (Federal

[58] Court of Appeal, [2002] *EWCA Crim* 747, paras. 2-4; Eur. Court H.R., *Perrin* (note 17).

[59] *Bundesgerichtshof, Toeben* (Federal Court), Judgment of 12 December 2000, case 1 StR 184/00, 46 *ENTSCHEIDUNGEN DES BUNDESGERICHTSHOFS IN STRAFSACHEN (BGHST)* 212 (2001) = 54 *NEUE JURISTISCHE WOCHENSCHRIFT* (*NJW*) 624 (2001), also available through http://www.bundesgerichtshof.de/.

[60] *Tribunal de Grande Instance de Paris, UEJF et Licra c/ Yahoo! Inc.*, Ordonnance de Référé of 20 November 2000, available at: http://www.juriscom.net/txt/jurisfr/cti/tgiparis20001120.htm; see also Joel R. Reidenberg, *Yahoo and Democracy on the Internet*, 42 JURIMETRICS JOURNAL 261 (2002).

[61] See the analysis given by KOHL (note 4), 47-65; from a perspective of private international law see ISABEL ROTH, *DIE INTERNATIONALE ZUSTÄNDIGKEIT DEUTSCHER GERICHTE BEI PERSÖNLICHKEITSVERLETZUNGEN IM INTERNET* 243-289 (2007).

[62] *Zippo Manufacturing Co. v. Zippo Dot Com Inc.*, US District Court for the Western District of Pennsylvania, 952 F.Supp. 1119, at 1124 (W.D.Pa. 1997); SCHMAHL (note 11), 306-307.

[63] See *Tribunal de Grande Instance de Paris, Yahoo* (note 60).

[64] See also *Bundesgerichtshof*, Judgment of 2 March 2010, case VI ZR 23/09, 63 *NEUE JURISTISCHE WOCHENSCHRIFT* 1752 (2010), para. 22 (also available through http://www.bundesgerichtshof.de/), where the German Federal Court emphasized that readers of the New York Times online edition could choose Germany in a list of countries of residence on registration.

[65] See KOHL (note 4) 97; see also Article 15(1)(c) Council Regulation (EC) 44/2001 of 22 December 2000 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters, O.J. L 12/1, according domestic courts jurisdiction over transnational consumer contracts if the other party "directs" commercial activities such as promoting websites to that state.

Court) could at least rely on the fact that Holocaust denial specifically affected Germany.[66] In Perrin, the offender was a UK resident, which established an additional link.[67]

In fact, jurisdiction based on an unqualified effects doctrine would not only infringe the sovereignty of other states, but it would also collide with the principle of internet freedom. Freedom of expression "regardless of frontiers", as laid down in Articles 19(2) CCPR and 10(1) ECHR, would come to an end if content providers had to block access for foreign users for fear of being sued or prosecuted abroad.[68] A fair balance must be struck between the conflicting principles of territorial jurisdiction and of internet freedom. From a human rights perspective it has been advanced that foreign jurisdiction must be foreseeable.[69] A qualified effects doctrine based on the idea of reasonableness comes to similar results.

II. The Country Code Top Level Domain as Cyberterritory

In IIL, the territorial principle undergoes a second change. In principle, territory is a land or sea space on the earth including the airspace above and the subsoil.[70] The internet has been assimilated to a territory where persons can act and even live. In 1996, John Perry Barlow emphatically declared the independence of cyberspace.[71] Barlow used the language of sovereignty and of the social contract[72] in order to argue that cyberspace was a "world" beyond state control. Meanwhile it has become clear that states are both willing and able to exercise jurisdiction over cyberspace. What is more striking is that parts of cyberspace seem to become part of state territory. Country code Top Level Domains (ccTLD) such as .uk for the United Kingdom and .pl for Poland may already be considered to be their respective states' cyber territories.

These Top Level Domains (TLDs) were created by Jon Postel, the father of the Domain Name System, who referred to a list of country codes established by the International Organization for Standardization.[73] He delegated the administration of the Top Level

---

[66] TOEBEN, (note 59), 46 BGHST 212, 224 (2001) = 54 NJW 624, 628 (2001).

[67] Eur. Court H.R., *Perrin* (note 20), Section The Law B.

[68] For a depiction of this scenario see KOHL (note 4), 279-283.

[69] Eur. Court H.R., *Perrin* (note 17), Section The Law B; KOHL (note 4), 115-163.

[70] See BROWNLIE (note 12), 105; DUPUY (note 10), para. 37.

[71] John Perry Barlow, *A Declaration of Independence of Cyberspace of 8 February 1996*, available at: http://w2.eff.org/Censorship/Internet_censorship_bills/barlow_0296.declaration; see also David R. Johnson and David G. Post, *Law and Borders – The Rise of Law in Cyberspace*, 48 STANFORD LAW REVIEW 1367 (1996).

[72] See the analysis given by ROLF H. WEBER, SHAPING INTERNET GOVERNANCE: REGULATORY CHALLENGES 73-88 (2010).

[73] Kleinwächter (note 3), 1106.

Domains to scientific or other institutions who were willing to act as registries. Since 1998, the creation and delegation of TLDs is the task of Internet Corporation for Assigned Names and Numbers (ICANN), a non-profit organization established under Californian law.[74] This is true of both ccTLDs and generic TLDs (gTLDs), such as .com or .info. CcTLDs therefore originate from a sphere that was hardly controlled by states. The British and the German ccTLD registries are still rooted in the private sector and both states limit control to a minimum. Other states such as France[75], however, effectively control their registries. This is also the case for the European Union which created its own ccTLD .eu by Regulation (EC) 733/2002 of the European Parliament and the Council.[76] The .eu registry, EURid, was designated upon a Call for Expressions of Interests[77] by the European Commission,[78] and it is bound by a service concession contract concluded by EURid and the European Commission.[79] By Regulation (EC) 874/2004[80] the Commission adopted public policy rules for the administration of the .eu ccTLD. The European Union thus claims full jurisdiction over the administration of its ccTLD.

This claim is supported by international documents. In principle, the creation and delegation of TLDs is still within the responsibilities of ICANN. The ICANN board is advised, however, by the Governmental Advisory Committee (GAC). Although the GAC is, formally speaking, an ICANN body established under its bylaws,[81] in reality it comes close to an international organization.[82] Recommendations adopted by the GAC are not formally

---

[74] See WEBER (note 72), 51-54.

[75] See Article L45, Articles R20-44-34-R20-44-41 *Code des postes et des communications électroniques* (Posts and Electronic Communications Code), consolidated version available through http://www.legifrance.gouv.fr/initRechCodeArticle.do.

[76] EP and Council Regulation 733/2002 of 22 April 2002, O.J. 2002 L 113/1.

[77] Commission, Call for Expressions of Interest for the Selection of the .eu TLD Registry, Notice of 3 September 2002, O.J. 2002 C 208/6.

[78] Commission Decision 2003/375 of 21 May 2003, O.J. 2003 L 128/29.

[79] See the draft service concession contract annexed to the Call for Expressions of Interests (note 77), at 14.

[80] Commission Regulation 874/2004 of 28 April 2004, O.J. 2004 L 162/40, last modified by Commission Regulation 560/2009 of 26 June 2009, O.J. 2009 L 166/3.

[81] ICANN, Bylaws as amended of 5 August 2010, Article XI(2)(1), available at: http://www.icann.org/en/general/bylaws.htm.

[82] See Wolfgang Kleinwächter*, Beyond ICANN vs. ITU: Will WSIS Open New Territory for Internet Governance?*, in INTERNET GOVERNANCE: A GRAND COLLABORATION (note 3), 31, 45; Uerpmann-Wittzack, (note 3), 160; for a concept to transform the GAC into an Internet Regulatory Organisation see Robert Uerpmann-Wittzack, *International Regulation by International Regulatory Organisations – A model for ICANN?*, THE GLOBAL COMMUNITY: YEARBOOK OF INTERNATIONAL LAW AND JURISPRUDENCE 2008, vol. I, 113 (2009).

binding upon the ICANN Board, it does "duly tak[e] into account"[83] recommendations of Governments who hold a de facto veto position.[84] In 2005 the GAC adopted the Principles and Guidelines for the Delegation and Administration of ccTLDs[85]. According to these Principles "[u]ltimate public policy authority over the relevant ccTLD rests with the relevant government". State sovereignty is thus affirmed.

The final documents of the World Summit on the Information Society (WSIS), which was held in two phases in Geneva 2003 and in Tunis 2005,[86] point in the same direction. Paragraph 63 of the Tunis Agenda for the Information Society of 18 November 2005 holds that:

> Countries should not be involved in decisions regarding another country's country code Top-Level Domain (ccTLD). Their legitimate interests, as expressed and defined by each country, in diverse ways, regarding decisions affecting their ccTLDs, need to be respected, upheld and addressed via a flexible and improved framework and mechanisms.[87]

A draft of 30 September 2005 went even further. It recognized "that each government shall have sovereignty over its respective country code top level domains."[88] While all the documents refer to the administration of ccTLDs, the underlying idea may be generalized: there is a genuine link between a ccTLD and the respective state. A state may therefore assert full jurisdiction over its own ccTLD. The ccTLD becomes a state's territory in cyberspace. The United Kingdom might therefore exercise criminal jurisdiction over any offence committed under its ccTLD .uk.

In summary, cyberspace does not defeat the principle of territorial jurisdiction. Rather, the principle adapts itself to the specific situation of the internet.

---

[83] Article I(2)(11) ICANN Bylaws (note 81).

[84] Kleinwächter (note 3), 1121-1122; Uerpmann-Wittzack (note 3), 156.

[85] Principles of 5 April 2005, available at: http://gac.icann.org/system/files/ccTLD_Principles_0.pdf.

[86] See WEBER (note 72), 31-36.

[87] Doc. WSIS-05/TUNIS/DOC/6(Rev.1)-E, available at: http://www.itu.int/wsis/docs2/tunis/off/6rev1.pdf.

[88] Doc. WSIS-II/PC-3/DT/10 (Rev.4)-E, para. 54; available at: http://www.itu.int/wsis/docs2/pc3/working/dt10rev4.pdf.

E. The Principle of Interstate Cooperation

In the field of internet governance, the need for international cooperation is above all a matter of fact. As the internet defies national borders, most problems cannot be solved by one state alone. For instance, internet fraud and other internet offences are frequently committed by offenders and through internet servers located outside the state of the victim. Prosecuting such offences requires investigations in different states which presuppose effective cooperation. The Convention on Cybercrime of 2001[89] is a result of this phenomenon, as it is grounded on the belief "that an effective fight against cybercrime requires increased, rapid and well-functioning international co-operation in criminal matters".[90]

The mere need to cooperate does not entail a legal obligation to do so. Certain duties to cooperate can be derived from general international law. For example, one of the purposes spelled out in Article 1 of the United Nations Charter is "To achieve international co-operation in solving international problems of an economic, social, cultural, or humanitarian character, and in promoting and encouraging respect for human rights and for fundamental freedoms". The Declaration on Principles of International Law concerning Friendly Relations and Co-operation among States in accordance with the Charter of the United Nations (Friendly Relations Declaration), which can be held to be an authoritative interpretation of the Charter,[91] confirms the duty of states to cooperate. However, this general obligation has a high level of abstraction, and it is difficult to translate it into specific duties.[92]

Specific duties to cooperate can be found in international treaties such as the Convention on the Rights of the Child (CRC).[93] Article 34(c) CRC obliges states to "take all appropriate national, bilateral and multilateral measures to prevent … [t]he exploitative use of children in pornographic performances and materials".[94] Since pornographic materials are frequently exchanged through the internet from one state to another, any effective response must be coordinated between two or more states. Thus, Article 34(c) CRC obliges

[89] Convention on Cybercrime, *supra*, note 53.

[90] Convention on Cybercrime, *supra*, note 53, Preamble, para. 8.

[91] Christoph Schreuer, *State Sovereignty and the Duty of States to Cooperate – Two Incompatible Notions?*, in INTERNATIONAL LAW OF COOPERATION AND STATE SOVEREIGNTY 163, 170 (Jost Delbrück ed., 2002); Philip Kunig, *United Nations Charter, Interpretation of*, in MPEPIL (note 22, 2006), paras. 12-14; see also Helen Keller, *Friendly Relations Declaration* (1970), in MPEPIL (note 22, 2009), para. 30.

[92] Schreuer (note 91), 170-174; see also VAUGHAN D. LOWE, INTERNATIONAL LAW 111 (2007).

[93] GA Res. 44/25 of 20 November 1989.

[94] *Id.*

states to cooperate in combating child pornography. In consequence, the Convention on Cybercrime, which defines offences related to child pornography in Article 9, expressly refers to the CRC.[95]

Similar obligations may follow from other human rights instruments such as the ECHR. In *Rantsev v. Cyprus and Russia* the European Court of Human Rights stressed the transnational character of trafficking in human beings. Therefore, the positive obligation to investigate cases of trafficking in human beings, deriving from ECHR Article 4, was understood to encompass a duty of effective cross-border cooperation.[96] The same should be true for offences through the internet which typically involve more than one state. If, for instance, in *K. U. v. Finland*[97] the internet dating site had been run by a provider outside Finland, the duty to protect the 12 year old boy under ECHR Article 8 would have implied an obligation to cooperate with the state where the provider was located.

However, there is no consistent pattern for duties to cooperate.[98] In fact, states are not even obliged to maintain diplomatic relations even though diplomacy is at the very basis of international cooperation. The final documents of the WSIS show the same ambivalence. The Geneva Declaration of 12 December 2003 concludes with a commitment "to strengthening cooperation to seek common responses to the challenges and to the implementation of the Plan of Action, which will realize the vision of an inclusive Information Society based on the Key Principles incorporated in this Declaration."[99] However, paragraph 40 of the Tunis Agenda[100] merely "underlines the necessity" to promote international cooperation. Although the need for cooperation is generally accepted, states are reluctant to accept such duties.[101] From a legal point of view, the principle of interstate cooperation is quite weak.

---

[95] 11th recital of the Convention's Preamble (note 53).

[96] Eur. Court H.R., *Rantsev v. Cyprus and Russia*, Judgment of 7 January 2010, Application 25965/04, para. 289.

[97] *K.U. v. Finland*, *supra*, note 49.

[98] But see Christian Tietje, *The Duty to Cooperate in International Economic Law and Related Areas*, in INTERNATIONAL LAW OF COOPERATION AND STATE SOVEREIGNTY (note 91), 45, 63-64: according to whom duties to cooperate are linked to issues of overlapping jurisdictions, which is indeed an important aspect; for different types of cooperation see Lori Fisler-Damrosch, *Obligations to Cooperate in the International Protection of Human Rights*, in INTERNATIONAL LAW OF COOPERATION AND STATE SOVEREIGNTY (note 91), 15, 24-30.

[99] Doc. WSIS-03/GENEVA/DOC/4-E, para. 65, available at: http://www.itu.int/dms_pub/itu-s/md/03/wsis/doc/S03-WSIS-DOC-0004!!PDF-E.pdf.

[100] Tunis Agenda, *supra*, note 87; see also *Id.*, paras. 47, 51, 69.

[101] For a pessimistic appraisal see KOHL (note 4), 251-252.

F. The Principle of Multi-Stakeholder Cooperation

Civil society and the private sector traditionally play an important role in internet governance. Although the development of the internet was funded by the US Government, its structures were determined by the scientific community. The US Government observed the development but it stayed in the background. When it became necessary to find stable structures for the administration of the internet Domain Name System (DNS), the task was neither conferred upon a state authority nor an international organization such as the International Telecommunications Union, but upon the private non-profit organization ICANN. Nevertheless, concepts of internet governance beyond state control such as the vision of John Perry Barlow in 1996[102] have never become true. ICANN has been under contract of the US Department of Commerce from the beginning.[103] Since then, the influence of other states has grown, and the Governmental Advisory Committee is now an important body of state control. Initial plans of the US Government to release ICANN into full independence have not yet been realized. The newly concluded Affirmation of Commitments by the United States Department of Commerce and the ICANN (Affirmation of Commitments) of 30 September 2009[104] further reduces direct US influence but enhances accountability and transparency by review procedures which involve, *inter alia*, the Governmental Advisory Committee. As early as in 2002 the President of ICANN called for "an effective public-private partnership, rooted in the private sector but with the active backing and participation of national governments."[105] This has been progressively realized.[106]

There are clear signs that this multi-stakeholder approach is not only a matter of fact but that it is perceived as a guiding principle of IIL. In the Affirmation of Commitments, the US Department of Commerce "affirms its commitment to a multi-stakeholder, private sector led, bottom-up policy development model for DNS technical coordination that acts for the benefit of global Internet users".[107] The subject was addressed in a broader context during

---

[102] Barlow, *supra*, note 71.

[103] See the Memorandum of Understanding of 25 November 1998 between the US Department of Commerce and ICANN, available at: http://www.icann.org/en/general/icann-mou-25nov98.htm; Dederer (note 3), 377-379 and 389-390, accentuates this form of state control.

[104] Available at: http://www.icann.org/en/documents/affirmation-of-commitments-30sep09-en.pdf.

[105] ICANN, President's Report: ICANN – The Case for Reform of 24 February 2002, available at: http://www.icann.org/general/lynn-reform-proposal-24feb02.htm.

[106] See also Kleinwächter (note 3), 1120-1123; Erich Schweighöfer, *Role and Perspectives of ICANN*, in INTERNET GOVERNANCE AND THE INFORMATION SOCIETY 79 (Wolfgang Benedek, Veronika Bauer & Matthias C. Kettemann eds., 2008).

[107] Affirmation of Commitments (note 104), para. 4.

WSIS. According to the Geneva Declaration of Principles of 2003, the management of the internet, which "encompasses both technical and public policy issues," "should involve all stakeholders and relevant intergovernmental and international organizations."[108] In this respect, the Declaration connects different actors with specific roles. Policy authority for internet-related public policy issues is ascribed to states[109] while the private sector shall have "an important role" in the technical and economic development of the internet.[110] The role of civil society is less specific. It shall play "an important role on Internet matters, especially at community level."[111] Two years later, the Tunis Agenda for the Information Society reaffirmed this multi-stakeholder approach in identical wording[112], it recommended a multi-stakeholder approach "at all levels",[113] and it created the Internet Governance Forum as a "new forum for multi-stakeholder policy dialogue".[114] This multi-stakeholder approach is not limited to questions of the Domain Name System and of ICANN. Rather, WSIS adhered to a broad notion of internet governance which includes public policy issues such as the prosecution of cybercrime.[115] In fact, cooperation between different stakeholders is a key note of the Geneva Declaration[116] and of the Tunis Agenda.[117]

The multi-stakeholder approach is not limited to ILL. Other world conferences also show a growing importance of non-state actors.[118] In IIL, however, the concept of multi-stakeholder cooperation is so strong that it takes the form of a well established principle.

---

[108] Geneva Declaration (note 99), para. 49.

[109] Geneva Declaration (note 99), para. 49(a).

[110] Geneva Declaration (note 99), para. 49(b).

[111] Geneva Declaration (note 99), para. 49(c) ; on the role of civil society within the WSIS process itself see Bart Cammaerts & Nico Carpentier, The Unbearable Lightness of Full Participation in a Global Context: WSIS and Civil Society Participation, in TOWARDS A SUSTAINABLE INFORMATION SOCIETY 17 (Nico Carpentier & Jan Servaes eds., 2006).

[112] Tunis Agenda (note 87), para. 35.

[113] Tunis Agenda (note 87), para. 37.

[114] Tunis Agenda (note 87), para. 72.

[115] See Tunis Agenda (note 87), paras. 40 and 56-62; see also the definition of internet governance given by the Report from the Working Group on Internet Governance of 3 August 2005, Doc. WSIS-II/PC-3/DOC/5-E, paras. 10-12, available at: http://www.itu.int/wsis/docs2/pc3/off5.pdf.

[116] Geneva Declaration (note 99), paras. 17, 20, 35, 60-61.

[117] Tunis Agenda (note 87), paras. 27(b), 39, 41, 45, 71, 83, 88-89.

[118] See Anna Spain, *Who's Going to Copenhagen?: The Rise of Civil Society in International Treaty-Making*, 13 ASIL INSIGHT No. 25 (2009), available at: http://www.asil.org/insights091211.cfm.

G. Interrelating Different Actors

The final documents of the WSIS enumerate states, the private sector, civil society and international organizations as key actors of IIL,[119] while individuals are the primordial actors in an order based on human rights. The five principles of IIL analyzed in this article determine the relationship between these actors.

Human rights protect individuals against interferences by public authorities. Both the freedom of communication and the privacy of individual communications are guaranteed. Whereas CCPR Article 1 Optional Protocol No. 1 only gives standing to human beings as such, European human rights may also be invoked by civil society or private sector actors formed out of individuals. This is spelled out in ECHR Article 34. The position of internet providers is further strengthened by World Trade Law.

Positive obligations deriving out of human rights norms regulate the relationship between different individuals, and by that define the position of individuals within civil society and towards the private sector. Above all, states are under an obligation to protect privacy against interferences by other individuals, civil society and the private sector. *K. U. v. Finland*[120] is a good example of this.

The principle of territorial jurisdiction aims at delimitating the powers of different states whereas cooperation is needed in order to resolve problems which cannot be handled by one sovereign state alone. Interstate cooperation is quite a traditional concept of international law even though the need to cooperate between sovereign states is particularly urgent in the field of internet governance. The concept of multi-stakeholder cooperation is more innovative, and it has become a specific principle of IIL. In short, IIL is currently evolving within a triangle of individual rights, territorial jurisdiction and cooperation.

[119] Geneva Declaration, *supra*, notes 108-111; Tunis Agenda, *supra*, note 112.

[120] *K. U. v. Finland*, *supra*, note 48.