The Jean Monnet Center for International and Regional Economic Law & Justice

THE NYU INSTITUTES ON THE PARK

THE JEAN MONNET PROGRAM

J.H.H. Weiler, Director

Jean Monnet Working Paper 24/14

Joanna Kulesza

Protecting Human Rights Online -- An Obligation of Due Diligence

NYU School of Law • New York, NY 10011
The Jean Monnet Working Paper Series can be found at
www.JeanMonnetProgram.org

ISSN 2161-0320 (online)
Copy Editor: Danielle Leeds Kim

New York University School of Law
New York, NY 10011
USA

Publications in the Series should be cited as:
AUTHOR, TITLE, JEAN MONNET WORKING PAPER NO./YEAR [URL]

PROTECTING HUMAN RIGHTS ONLINE -- AN OBLIGATION OF DUE DILIGENCE

By Joanna Kulesza[*]

Abstract

This paper covers the challenge of effective human rights protection online. It argues that international law provides sufficient background to identify the limits of states' obligations to protect human rights in cyberspace. Referring to the work of the United Nations (UN) Human Rights Committee (HRC) and UN Special Rapporteurs the author answers pressing international law questions on limits of privacy and freedom of speech in the transboundary cyberspace. The current work emphasizes states' positive obligation to actively protect rights of individuals within their jurisdiction, power or control and points to the due diligence standard enshrined in international law on state responsibility and international liability as validation for the prerequisite of state efforts aimed at protecting individuals from human rights violations online coming from any third party.

[*] Email: joannakulesza@gmail.com

1. International law and the Internet – from Internet governance to international Internet law

The global network or interconnected devices operating on the TCP/IP protocol or ones compatible therewith may be referred to as the Internet.[1] The sci-fi literature originated term "cyberspace" has come to signify the platform of human-computer interaction enabled by the TCP/IP interconnected devices.[2] With almost 40% of world's population using the Internet in 2013[3] the question of individual rights and obligations is forever more pressing. It might seem that almost 70 years of human rights law development would allow the international community for a relatively easy transition from its off-line to an online application, yet that is not the case. Practical questions on limits of state surveillance for reasons of personal privacy or the applicability of varying national laws on defamation online have shown that practical, universal criteria for effective human rights protection are needed rather than a broadly defined, political compromise, dominating the human rights debate so far.

Human rights are however not the only domain of international relations and international law significantly altered by the characteristics of cyberspace. The Internet changed more than just the perception of human rights. With its decentralized nature and multistakeholder governance it also altered the role of states when it comes to protecting human rights. While within their "physical" territories states act through law

[1] As Tim Wu puts it, the TCP/IP can be considered the Esperanto for computers. Tim Wu, The Master Switch 196 (2010).

[2] The term „cyberspace" first appeared in William Gibson's 1984 sci-fi novel „Nerumaoncer" where it was described as „a consensual hallucination experienced daily by billions of legitimate operators, in every nation (...). A graphic representation of data abstracted from the banks of every computer in the human system". William Gibson, Neuromancer, (1984) at 67. While the term has come to signify many different notions since then a legal definition of cyberspace is hard to find. Poland, included such a unique defintion in one of its recently ammended acts of law. According to Article 2 para. 1b of the Act of August 29, 2002 on martial law and the competences of the General Commander of Armed Forces and principles of his subordination to constitutional Polish authorities (ustawa z dnia 29 sierpnia 2002 r. o stanie wojennym oraz o kompetencjach Naczelnego Dowódcy Sił Zbrojnych i zasadach jego podległości konstytucyjnym organom Rzeczypospolitej Polskiej) According to this act cyberspace is to be understood as the space of processing and exchanging information "created by teleinformation systems", including their interconnections and relationship with users. The amended act allows the General Commander to introduce martial law in case of threats to Poland's security originating "from cyberspace". Contrary to Poland however, most states are reluctant to codify the definitions of "Internet" or "cyberspace" as the notion evolves quickly, following the fast paced technological revolution we face every day.

[3] International Telecommunications Union (ITU), The World in 2013: ICT Facts and Figures, Geneva 2013, 2, available at: http://www.itu.int/en/ITU-D/Statistics/Pages/facts/default.aspx.

enforcement agencies, online they need the necessary help of Internet service providers (ISPs) – companies or individuals hosting websites or rendering services, including those consisting of enabling Internet access – to be able to execute their powers and enforce their laws. With the transnational character of the network and ISPs located in various jurisdictions, offering their services worldwide, states find it forever more difficult to effectively execute their laws within their national territories when it comes to online infringements or law violations. Often the help of foreign private bodies is a necessary prerequisite for having taken offline e.g. content defamatory according to national laws. As the case of the redwatch.org site shows, since 2006 Poland has been unable to make the U.S. located .org registry, a Virginia based company named VeriSign, take down the xenophobic and racist content of the Polish-language right-extremist website, encouraging violence against racial and religious minorities in Poland. Since the content of the website falls within the U.S. First Amendment, neither the U.S. based company, nor U.S. authorities have legal grounds for taking it offline. Poland is therefore unable to cause for the content that is contrary to Polish law to disappear from the Internet, while blocking access from within state territory to any information, whether illegal or not, is not provided for by Polish law. This Polish case is obviously not unique. Without enhanced international cooperation it is impossible to shape the scope of human rights online, be it freedom of speech, non-discrimination or privacy. Enhanced international cooperation regarding the online environment refers however not only to state parties. ISPs play a crucial role in protecting or limiting human rights online, adding to the debate on the human rights obligations of global corporations.[4]

[4] See: United Nations Guiding Principles on Business and Human Rights, 2011, also known as „Ruggie Principles" after their author, John Ruggie, United Nations Secretary-General's Special Representative for Business and Human Rights from 2005 untill 2011; The Guiding Principles on Business and Human Rights: Implementing the United Nations 'Protect, Respect and Remedy' Framework, UN Doc. A/HRC/17/31, 21 March 2011. The Principles refer to three basic tools aimed at ascertaining human rights enforcement vis-a-vis transnational companies. Those include states' obligation to protect human rights, corporate responsibility for their protection and the accessibility of a legal remedy for victims of abuses caused by companies. Contemporary international law does not permit putting international obligations directly onto private parties, therefore it is states who are obliged to assure that private companies operating under their jurisdiction, power or control meet human rights standards set by international law. This debate gained most media attention in recent years with the increased controversies over actions of private military firms deployed by states in regions of internal turmoil or international conflict. See generally e.g.: Anna Leander, *The Market for Force and Public Security: The Destabilizing Consequences of Private Military Companies*, 5(42) Journal Of Peace Research 605 (2005), at 605-622.

The unique characteristic of managing the global digital resource that is the cyberspace has come to the attention of the international community no sooner than 2003 and is referred to with the term "Internet governance".[5] In 2003 the UN International Telecommunications Union (ITU) called upon states to participate in the first World Summit on the Information Society (WSIS). Its aim was to identify crucial challenges to managing the network and provide recommendations on its future administration. The WSIS called upon a group of experts within the Working Group on Internet Governance (WGIG) who presented their report to member states. The WGIG suggestions were included in the 2005 Tunis Agenda for the Information Society, a document considered a milestone in the development of Internet governance, containing basic principles of this area of international relations. According to the Tunis Agenda "Internet governance" is "the development and application by governments, the private sector and civil society, in their respective roles, of shared principles, norms, rules, decision-making procedures, and programmes that shape the evolution and use of the Internet".[6] This concise definition is a good reflection of the specifics of Internet architecture, that is perceived as a layered structure. The Internet may be generally envisaged as comprised of at least three concentric layers: most central physical layer of hardware and telecommunication wires, middle layer of code, including software and allowing the hardware to engage in communication and the outer content layer, where information and services are provided and shared with the use of the hardware and software.[7] Each of the layers is governed by different group of entities. While the elements of the physical layer belong to companies, usually privately owned telecommunication operators, the software layer (or the layer of code) is developed by individuals, usually computer scientists, within few self-governing informal forums, such as the Internet Engineering Task Force (IETF) or the World Wide Web Consortium (W3C). The

[5] On the genesis of the notion and its potential misundestanding see: Milton Mueller, Networks and States, The Global Politics of Internet Governance (2010), at 8-9.

[6] Paragraph 34, World Summit on the Information Society, Tunis Agenda for the Information Society, Tunis 2005, available at: https://www.itu.int/wsis/docs2/tunis/off/6rev1.html. The term "respective roles" is subject to most controversy when interpreting the definition, as in practical terms it is difficult to distinguish the roles of individual stakeholders, e.g. the limits of ISP responsibility for enforcing national legal standards – those would be perceived differently in e.g. Europe and Asia. See e.g. Milton Mueller, John Mathiason and Hans Klein, The Internet and Global Governance: Principles and Norms for a New Regime, 13 GLOBAL GOVERNANCE, 237, 241 – 242 (2005).

[7] For more on this distinction see: Joanna Kulesza, International Internet Law (2012) at 126.

specifics of such standard setting bodies and, accordingly, the organization of this middle, code layer is a direct consequence of the network's genesis – what once was a strictly academic exercise remains strongly influenced by computer science scholars, seeking most effective ways to relay packets of data, less mindful of national or international policies and power struggles. Technical standard setting stays therefore out of the hand of states or companies alike, as a non-policy matter.[8] The role of state authorities is strongest in only one of the three, complementary layers – the layer of content. States wish for the content available within their territories to adhere to local laws and try to influence the scope of information available online through the execution and enforcement of national laws. Yet they often fail, due to the fact that all the layers are strongly interconnected - it is impossible to effectively manage one of them without the necessary influence with others. It is impossible to rule the content alone, since it runs on code, created by individuals in non-governmental forums and is conveyed through privately owned networks or underwater cables.[9] As much as states had the authority and the physical capability to confiscate an entire printed edition of a newspaper containing a defamatory statement, they often cannot physically stop an online publication, even though it is available within their territories. This unique, transnational specific of the cyberspace requires an effective cooperation of all stakeholders, a characteristic of Internet governance referred to as a principle of multistakeholderism and worded in the Tunis Agenda quoted above, referring to three groups of stakeholders: the private sector running the hardware, civil society, including academia, designing the code and states, applying their laws over online content and its authors or users.

[8] Although, as already mentioned, the distinction between policy and non-policy matters may be considered vague, see supra 8. The current political debate over internationalisation of the U.S. based Internet Corporation of Assigned Names and Numbers (ICANN), supervising the technical coordination of basic Internet resources, reflects this dogmatic challenge. See e.g. European Commission, Commission to pursue role as honest broker in future global negotiations on Internet Governance, Feb. 12th, 2014, IP/14/142, available at: http://europa.eu/rapid/press-release_IP-14-142_en.htm.

[9] The recent NSA scandal, where US agencies deployed deep-pocket inspections and underwater cable surveillance to gather intelligence information on all Internet users of US based telecommunication services, shows perfectly how futile (as the endeavor failed causing diplomatic and political outrage) and legally challenging (since the US violated human rights of non-state individuals) state's intended influence in all three layers is.

The need for multistakeholder cooperation is particularly well visible when it comes to protecting human rights online. With the need to identify individual obligations of states towards all Internet actors – users and ISPs alike – the time seems ripe to introduce legal obligations, derived from international human rights law developed so far, to the online environment. While there is a strong background in international law of contracts and jurisprudence, all the human rights principles need to be applied "appropriately" to reflect the specifics of this unique medium they are to govern. With that in mind the basic principles of what might be called an international Internet law may be identified. They reflect the soft law specifics of Internet governance, as drafted by the WSIS in its 2005 Tunis Agenda, with its governing principle of multistakeholderism, requiring multistakeholder cooperation in all areas of Internet-based interaction, taking the leading power off states, dividing it instead among all three groups of stakeholders. International Internet law principles include, next to multistakeholderism, cultural diversity, freedom of access, openness and network security.[10] From those general principles detailed obligations, referring to e.g. individual privacy or freedom of speech can be identified, based on the body of international human rights law. With the multistakeholderism principle in mind, detailed obligations of all stakeholders in the domain of human rights protection may be drafted as an act of international law. Elements of international law obligations specific to the cyberspace environment, based on the WSIS work, are reflected in the rich body of Internet governance scholarship and in recent works of intergovernmental organizations, such as the Council of Europe with its non-binding Declaration by the Committee of Ministers on Internet governance principles[11] as well as individual states, following the lead of Brazil,[12] discontented with the US cyber espionage laws behind the NSA controversy, recognizing it a grave violation of international human rights law in need of a reaction from the international community. It is Brazilian President Rousseff calling for setting a clear sequence of

[10] For a detailed analysis of the international Internet law principles see: Joanna Kulesza, *International Internet law*, 24(3) Global Change, Peace & Security 351 (2012), at 351 – 364.
[11] Declaration by the Committee of Ministers on Internet governance principles, adopted by the Committee of Ministers on 21 September 2011 at the 1121st meeting of the Ministers' Deputies.
[12] See: Contribution from the Federative Republic of Brazil, Draft Opinion on the Role of Government in the Multistakeholder Framework for Internet Governance, submitted for the fifth World Telecommunication/ICT Policy Forum, Geneva, 2013, available at: http://www.itu.int/md/dologin_md.asp?lang=en&id=S13-WTPF13-C-0005!!MSW-E.

internationally enforceable Internet governance principles serving as the foundation of all national legislature influencing the operation of the global communications network and her voice is being heard by European and American states.[13] The route towards a single international law document, initially containing soft law Internet governance principles, eventually following the path of international environmental law, a well established domain of international public law, has been instigated.

The legal enforceability of such principles can be easily derived from the international law obligation of states to prevent any human rights violations within their jurisdiction, power or control, where the international due diligence standard shall serve as a measure for identifying the scope of efforts required of each individual state party. Reflecting the development of human rights law obligations of transnational companies, as described in the Ruggie Report, ought to be considered the required code of conduct for international corporations. Their enforcement should be left to international organizations, such as the WTO or the ITU within their internal arbitration forums. The example of arbitration courts for domains names, hosted jointly by the World Intellectual Property Organization (WIPO) and ICANN based on their jointly developed Uniform Domain-Name Dispute-Resolution Policy (UDRP)[14] shows the perfect example of effective arbitration taking over where national intellectual property laws fell short.

2. The notion of human rights

The concept of human rights has been maturing together with the international community. With racial and sexual prejudice perceived as the acceptable standard until 20th century, it was primarily through the intense work of world's great thinkers and activists that a universal perception of human rights, granted to all individuals as a manifestation of their dignity found its way into international treaties, national acts of law and local courtrooms. What seemed incomprehensible to the greatest minds of the

[13] See the contributions to the NetMundial – Global Multistakeholder Meeting on the Future of Internet Governance, April 2014, http://content.netmundial.br/docs/contribs, in particular the one from Germany: German Government Proposal on Global Internet Principles, available at: http://content.netmundial.br/contribution/german-government-proposal-on-global-internet-principles/32.

[14] ICANN, Uniform Domain Name Dispute Resolution Policy, adopted August 26, 1999, available at: http://www.icann.org/en/help/dndr/udrp/policy.

18th century, like e.g. Thomas Jefferson – a human rights architect, doubtful of successful abolition of slavery and a slave owner himself - is considered the basis of international consensus two centuries later.[15] As the evolution of human rights unfolds, forever new values, such as environmental or sexual rights are reflected in its scope.

This evolution, first recognized by the international community of states within the 1948 Universal Declaration of Human Rights (UDHR), may be explained through the concept of human rights categories.[16] The very basic compromise on rights pertinent to every human being, expressed in the UDHR and the following international treaties, is perceived to include two differing categories of human rights, while the human rights ideology emphasizes their indivisibility.[17] Their very allocation within separate international treaties in 1966: the International Covenant on Civil and Political Rights (ICCPR) and the International Covenant on Economic Social and Cultural Rights (ICESCR) reflects the differing nature of particular rights. Economic, social and cultural rights listed in the ICESCR are considered to be positive, resource-intensive, progressive, vague, political (ideologically divisive), socialist and non-justiciable, making them rather aspirations or goals, then "real" legal requirements. At the same time civil and political rights, enumerated in the ICCPR are considered negative in character - requiring a state to allow for certain individual liberties rather then provide additional resources or services, cost-free, immediate, precise, non-ideological (non-political), capitalist, justiciable and therefore considered real "legal" rights.[18] Therefore human rights ideology conditions the fulfillment of the second group of rights, the so-called rights to subsistence from the provision of rights identified as being in the first

[15] See e.g.: J. Horton, L. Horton, Slavery and Public History: The Tough Stuff of American Memory, UNC Press Books 2009, p. vii; as Jefferson wrote "we hold these truths to be self-evident, that all men are created equal" he owned at least 150 slaves.

[16] The author internationally does not refer to the idea of human rights generations, as they do not seem to reflect the current evolution of this group of international law's development. For the discussion on the three generations of human rights see e.g.: Christian Tomuschat, Human Rights: Between Idealism And Realism (2008) at 25-38.

[17] See e.g.: Vienna Declaration and Programme of Action, Adopted by the World Conference on Human Rights in Vienna on 25 June 1993, which states that "all human rights are universal, indivisible and interdependent and related. The international community must treat human rights globally in a fair and equal manner, on the same footing, and with the same emphasis".

[18] Craig Scott, Interdependence and Permeability of Human Rights Norms: Towards a Partial Fusion of the International Covenants on Human Rights; 27 OSGOODE HALL LAW JOURNAL 769, 769 (1989).

generation.[19] Recent developments in international law invited the idea of a third category of human rights, which include e.g. environmental rights, such as the right to a healthy or adequate environment or sexual rights. The latter include Lesbian, Gay, Bisexual, Transgender (LGBT) rights identified in the 2007 Yogyakarta Principles, followed by the 2008 UN General Assembly Declaration on sexual orientation and gender identity.[20] The Declaration was supported by 67 member states and opposed by 57, clearly depicting the disparity in understanding the modern concept of human rights. Also within that category reproductive rights may be named, including a right to abortion confronted with the well-established right to life. The philosophical debate on the beginning of one's right to life – whether it is granted upon live birth, upon obtaining the capability to physically sustain living function or upon conception - influences strongly differing national policies and fuels an emotional debate on values and morality.

Third group of rights may therefore be derived from other human rights e.g.: right to life, right to health or the right to private and family life. It includes also the right to communication, originating from the well-established right to freedom of expression.[21]

What may be referred to as a new, fourth group of human rights might include those rights that are derivative of one of more rights from the groups already developed.[22] The right to Internet access falls into this category, possibly next to the recently much discussed right to be forgotten[23] or the proposed right to virtual personality.[24]

---

[19] See e.g.: Alison Brysk, Globalization And Human Rights (2002) at 78 – 79.
[20] UN General Assembly, Statement on Human Rights, Sexual Orientation and Gender Identity, 18 December 2008, A/63/635.
[21] See e.g.: Richard Pierre Claude And Burns H. Weston, Human Rights In The World Community: Issues And Action (2006) at 26.
[22] Nicola Lucchi, *Access to Network Services and Protection of Constitutional Rights: Recognizing the Essential Role of Internet Access for the Freedom of Expression*, 19(3) Cardozo Journal of International And Comparative Law, available at http://www.cjicl.com/uploads/2/9/5/9/2959791/cjicl_19.3_lucchi_article.pdf (2011).
[23] The „right to be forgotten" has been included in the proposed reform of EU data protection laws, see: Article 17, European Commission, Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), Brussels, 25.1.2012, COM(2012) 11 final, available at: http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf. Article 17, entitled „Right to be forgotten and to erasure" obliges data controllers to "take all reasonable steps, including technical measures, (…), to inform third parties" processing data requested by the subject

Consequential of the right to free expression, or more directly derived from the right to receive and impart information, as elementary for freedom of expression, it is funded on the conviction that the Internet has become one of the most significant tools for human interaction, and as such the primary source of information and knowledge. Limiting or denying access to the network equals limiting or denying access to information and the ability to share one's views freely. The right to internet access may be perceived as an element of the need to protect the substantial integrity of human rights.

The French Constitutional Council was confronted with the question of Internet's access as a human right in 2009 with regard to copyright protection granted in French law.[25] The 2009 Loi n°2009-669 du 12 juin 2009 favorisant la diffusion et la protection de la création sur internet (also called « loi Hadopi") introduced the *Haute Autorité pour la Diffusion des Œuvres et la Protection des Droits sur Internet* (HADOPI) – an administrative body authorized to disallow Internet access to individual users who breached national copyright regulations despite previous warnings (the so-called three strikes law). According to its original wording, assessed by the Constitutional Council, the decision to disallow Internet access was to be made by an administrative body (HADOPI) with no judicial supervision. What followed was a constitutional complaint based on the right to free speech, and in particular the right to access information. The claimants argued that "by giving an administrative authority, albeit independent, the power to impose penalties in the form of withholding access to the internet, Parliament firstly infringed the fundamental right of freedom of expression and communication,

---

to be removed, "that a data subject requests them to erase any links to, or copy or replication of that personal data". The Regulation forms thereby a best efforts obligation on the side of the data controlled, based on a due diligence test and derived from the right to erasure, well-present in EU law, rather than an executable right to "be forgotten" i.e. to have one's data effectively removed from the web.

[24] Proposed for, yet eventually not directly recognized in the constitution of Costa Rica in 2005, see: William Heath, *Costa Rica creates new human rights for your digital persona*, Ideal Government, 17 May 2005, available at: http://idealgovernment.com/2005/05/costa_rica_creates_new_human_rights_for_your_digital_persona/. On the right to virtual personality as a personal right according to German civil law see generally: Julia Meyer, Identität Und Virtuelle Identität Natürlicher Personen Im Internet (2011).

[25] French Constitutional Council: Decision n° 2009-580 of June 10th 2009—Act furthering the diffusion and protection of creation on the Internet, 10 June 2009; English translation available at: http://www.conseil-constitutionnel.fr/conseil-constitutionnel/root/bank/download/2009-580DC-2009_580dc.pdf.

and secondly, introduced patently disproportionate penalties."[26] According to the Council "the powers to impose penalties [...] vest [HADOPI], which is not a court of law, with the power to restrict or deny access to the internet by access holders and those persons whom the latter allow to access the internet" and therefore could lead "to restricting the right of any person to exercise his right to express himself and communicate freely, in particular from his own home" contrary to the freedom of expression guarantee in Article 11 of the French Constitution, holding respective provisions of the act unconstitutional. The Council's decision was interpreted as confirming the right to Internet access.[27] Eventually the entire act was reverted by the French parliament in 2013 as excessively restrictive upon individual rights,[28] yet the debate on the existence of a human right to Internet access and on human rights protection in cyberspace goes on.

In summary one may recognize the right to Internet access as a new, specific human right, one necessitating freedom of expression, including the right to receive information, in the 21st century. Limiting or depriving of Internet access directly influences the scope of enforceable freedom of expression. As a side note one might consider such a conclusion as a strong addition to the significance of UN initiatives aimed at fighting the digital divide[29] or the discussion on the necessary reform of copyright, which in its present form effectively limits fair use, designed for the very purpose to share and build upon past developments.

---

[26] Idem, p. 3-4.

[27] See e.g.: Richard Wray, *French anti-filesharing law overturned*, The Guardian, 10 June 2009, available at: http://www.theguardian.com/technology/2009/jun/10/france-hadopi-law-filesharing?guni=Article:in%20body%20link.

[28] Décret n° 2013-596 du 8 juillet 2013 supprimant la peine contraventionnelle complémentaire de suspension de l'accès à un service de communication au public en ligne et relatif aux modalités de transmission des informations prévue à l'article L. 331-21 du code de la propriété intellectuelle; available at: http://www.journal-officiel.gouv.fr/publication/2013/0709/joe_20130709_0157_sx00.html?verifBaseDir=/verifier&notVerif=0&verifMod=load.php&verifExplMod=attente.php&ficBaseDir=../publication/2013/0709&joDate=09/07/2013#test60

[29] See e.g. Jeffrey James, *Digital Divide Complacency: Misconceptions and Dangers*. 24 The Information Society 54 (2008), at , 54-61.

3. Human rights online

As the latest NSA surveillance affair showed, the power to abuse individual human rights online, in this case the right to privacy, no longer rests exclusively in the hands of governments.[30] It is only with the help of ISPs like Google, Microsoft, Facebook or Yahoo, who offer their services to millions of users from various jurisdictions and of differing nationalities, that a state – in this case the U.S. - may exercise its national laws. At the same time the transboundary character of the network makes it technically much easier to invade individual rights – be it through automatic collection of digitized data, intercepting online communications or disabling access to particular content.[31] Those specifics require to readapt the human rights framework, aimed primarily at state parties, for the multistakeholder environment that is the cyberspace. As challenging as that may sound, the international community has been at the attempt to involve private business into human rights protection for more than half a century – it was the rise of international environmental law that called for the enhanced public-private cooperation in order to protect the environmental rights of individuals.[32]

Deriving from the international environmental law experience a set of guidelines for online businesses, i.e. ISPs, allowing them to identify their human rights obligations, ought to be identified. In order for that to be possible, the human rights catalogue, as recognized before the rapid development of online communications, that is until early 1990s (in 1991 the U.S. National Science foundation enabled the commercial use of the initially academic network, causing for the "dotcom bubble" to grow) must be reanalyzed with the context of human rights application in the transboundary cyberspace.

Numerous attempts at that endeavor have been made by civil society, international organizations and individual states. They all provide practical interpretations of the

[30] Barton Gellman, Laura Poitras, *U.S., British intelligence mining data from nine U.S. Internet companies in broad secret program*, Washington Post, June 6, 2013 available at: http://www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story.html.
[31] See supra 33 on the technologies deployed by the NSA.
[32] See supra 6.

broad human rights catalogue in light of existing scholarly writing and jurisprudence set against the background of Internet governance practice and principles.

Among the civil society initiatives the most elaborate one is an attempt by a working group initially funded for the Internet Governance Forum, presently operating as an "open network" comprised of "of individuals and organizations (…)committed to making the Internet work for human rights".[33] Their 10 Internet Rights and Principles are the most concise proposal for reintroducing human rights for the online environment. While strongly rooted in the international human rights law and based on a thorough analysis of the existing documents and accompanying soft law, the proposal reflects the needs of online interactions. The 10 basic principles reflecting human rights needs of the online environment include 1) above all the need for universality and equality for all human rights, both online and offline; 2) respect for human rights and social justice; 3) accessibility, as the basic prerequisite for human rights protection online – as already mentioned, Internet access is the precondition for all other human rights exercised online, while according to the IRP principles, such access should be accompanied by the right to use the network in a "secure and open" manor; 4) as a consequence of nondiscriminatory access to the network, all of its users need to be able to express themselves freely, exercising the three composite freedoms included in the human rights regime: the right to hold, impart and receive information, without interference or censorship; 5) an individual rights that enjoys a high position on the list is privacy – in its online version it ought to be accompanied by effective personal data protections, granting freedom from surveillance, the right to use encryption and the right to online anonymity, signifying the right to use technical tools available to conceal one's identity. The list of online human rights includes also 6) the individual right to life, liberty and security, although the first one is rarely under a direct threat from online activites; the IRP Coalition puts emphasis on the need to protect those rights from infringements through, e.g. the exercise of other rights, such as the right to free speech, taking on the form of hate speech, inciting racial or religious hatred or encouraging to genocide; 7) for human right to be respected in the universal online environment they must be

[33] See IRP homepage at: http://internetrightsandprinciples.org/site/.

accompanied by respect for and promotion of cultural and linguistic diversity , in particular through "technical and policy innovations"; 8) a human rights specific for the online environment is referred to as "network equality" signifying the right to "universal and open access to the Internet's content, free from discriminatory prioritization, filtering or traffic control on commercial, political or other grounds". Another cyberspace-specific right is a right of 9) non discriminatory technical regulation of online resources, a result of the layered Internet structure, referred to hereinabove. The IRP proposal includes a right referring to "Internet's architecture, communication systems, and document and data formats" that ought to be "based on open standards", ensuring "complete interoperability, inclusion and equal opportunity for all". This proposal ought to be seen as reference to the need of ensuring human rights online not just through political or legal means, but also through technical ones, fundamental to Internet's functioning. Interference with the latter is bound to shape the former – in the online environment any such modification must ensure equal and non-discriminatory access to all Internet's resources, in order to avoid discrimination based on economic or technological status. Eventually 10) the charter refers to human rights as the foundations of all Internet governance – since it is the global community that is to be governed the existing human rights compromise, reflecting the different facets of human dignity, must lie at its foundations. Such a compromise must be identified and enforced through a multistakeholder cooperation.[34] The IRP Coalition is a world-wide endeavor, yet its management and roots lie in Europe, with European civil society activists and academics paving the way and strongly influencing the final shape of the document.

Another civil society proposal, offered by the Association of Progressive Communications – a non-profit funded by the Swedish International Development Cooperation Agency and resourced by civil society activists and academics from New Zealand and the US aims for the same goal and much similar in content to the IRP,

[34] The 10 Internet Rights and Principles proposal is available at: http://internetrightsandprinciples.org/site/wp-content/uploads/2014/03/IRP_booklet_6March2014_10principles.pdf.

although differently organized.[35] The proposal is focused around 7 themes that reflect: 1) the need for universal Internet access "for all"; 2) freedom of expression and association to be granted online as it is offline; 3) access to knowledge, reflecting the need to preserve network neutrality and as well as fair use and freedom of information, including the right to share and access it 4) consequentially a direct reference to the need to further develop free and open source software as a guarantee for "shared learning and creation"; 5) the need for online privacy and the right to protect it through electronic means, such as encryption software; 6) the necessity to use human rights as basis for all Internet governance related activities, in particular the neutrality of its standard setting and multistakeholder oversight of all governance activities. Eventually the charter calls for enhanced dissemination of information on the scope of online rights, derived from human rights law and emphasizes the need to introduce effective enforcement measures vis-à-vis human rights violations online.[36]

Third interesting example of civil society attempts to introduce human rights online is a Brazilian initiative of a crowd-sourced bill, to be introduce by Brazilian lawmakers through a fully democratic, yet technology-supported mechanism. The Marco Civil da Internet, initiated in 2009 by the office of Legislative Affairs of the Brazilian Ministry of Justice together with the School of Law in Rio de Janeiro at the Getulio Vargas Foundation, was proposed in 2011 by President Rousseff for parliamentary consideration as part of bill PL 2126/2011.[37] Even though in 2013, after the NSA cybersurveillance affair the President officially gave the bill the status of urgency, work over its further adoption was suspended in October 2013, but talk on relaunching the legislative procedure did not seize.[38] The proposed act 2126/11 includes 25 articles divided into 5 chapters that cover: 1) introductory regulations, 2) a unique lists of rights

[35] APC Internet Rights Charter is available at: http://www.apc.org/en/system/files/APC_charter_EN_0.pdf.
[36] APC Internet Rights Charter, pts 7.1. – 7.2 available at: http://www.apc.org/en/system/files/APC_charter_EN_0.pdf.
[37] Project de Leu No 2.126, de 2011, available at: http://www.camara.gov.br/internet/agencia/pdf/Emenda_aglutinativa_N_1.pdf .
[38] E. Piovesan, Plenário poderá discutir marco civil da internet na semana que vem, official website of the Chamber of Deputies (Camara des Deputados) of the Brazilian Parliament, March 14, 2014 available at: http://www2.camara.leg.br/camaranoticias/noticias/POLITICA/463648-PLENARIO-PODERA-DISCUTIR-MARCO-CIVIL-DA-INTERNET-NA-SEMANA-QUE-VEM.html.

of users and Internet-specific definitions, 3) rights and obligations of online services providers, 4) rules of effective online governance and 5) a set of final regulations. It identifies Internet access as the necessary precondition for the full enjoyment of human rights in the information society.[39]

Following the Brazilian example other states introduced similar initiatives, with the 2012 crowd-sourced Magna Carta for Philippine Internet Freedom, which has by now passed the first reading in the parliament.[40]

All the proposals share one common feature – they introduce a new model of drafting legal acts, one based on online community involvement, open to civil society input, reflecting the needs and hopes of community members. They reflect the well established catalogue of human rights, yet amend it through introducing news, cyber-specific elements, such as the need to make Internet governance a multistakeholder process and guarantee its neutrality through both: democratic procedures and technical standards. They emphasize directly two rights, particularly significant for online communications from among the human rights catalogue: the right to freedom of expression, including the right to distribute ideas, also anonymously and access information without censorship as well as the right to privacy, including freedom from surveillance.

The reassessment of human rights for the online environment has however not been done solely by civil society and NGOs. Also international tribunals and organs are involved in this process.

4. United Nations work on human rights online

The key challenges, when it comes to online communications, faced by the international community in general and international tribunals in particular, is the confrontation of equal values presented by individual privacy and collective security on one hand and freedom of expression set against national obscenity of libel laws on the other. As long

[39] Article 7, Project de Leu No 2.126, de 2011, available at: http://www.camara.gov.br/internet/agencia/pdf/Emenda_aglutinativa_N_1.pdf.
[40] 16th Congress of the Republic of the Philippines, Senate Bill No. 1091, introduced by Sen. P. P. Aquino, July 24, 2013, available at: http://202.57.33.10/plis/data/1712414352!.pdf.

as the former challenge remains unsolved, the latter one seems to be slowly unraveled by international tribunals and national legislature, introducing forever more detailed regulations on Internet filtering and notice-and-takedown procedures.

When it comes to privacy, while one of the earliest UN documents on the issue relating to telecommunication networks - the 1988 UN Human Rights **Committee** Recommendations on privacy - is still directly applicable to online challenges, in particular in the light of the recent NSA surveillance controversy,[41] the case of online freedom of expression seems somewhat more challenging. Both those issues are discussed in more detail below.

4.1. Privacy v. security

Privacy holds a well-established place in the human rights catalogue, with Article 12 of the UDHR or Article 17 of the ICCPR granting every individual freedom from "arbitrary interference" with their "privacy, family, home or correspondence" as well as from any "attacks upon his honour and reputation", placing privacy among the catalogue of personal rights known to every national legal system. The UN devoted much attention to individual privacy protection while discussing the issues of terrorist prevention. As Special Rapporteur on human rights and terrorism, M. Scheinin, rightfully notes, it was the war on terrorism that lead to a speedy erosion of the right to privacy.[42] The reason for this was primarily the inherent deficiency of Article 17 ICCPR, granting the individual right to privacy: the lack of a limitative clause requiring states to meet three basic criteria: the necessity, proportionality and reasonableness of the interference yet argues that its very context introduced such an obligations resting upon states. The contents of such an obligation and the limits of individual privacy permissible under international human rights law are the core of the challenge posed by online communications, since, as already mentioned above, the global online community needs a global privacy standard for its protection to be truly effective.

[41] UN Human Rights Committee General Comment No. 16: Article 17 (Right to Privacy), The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation, 8 April 1988, available at: http://www.refworld.org/docid/453883f922.html.
[42] Human Rights Council, Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, Martin Scheinin, Dec. 28, 2009, U.N. Doc. A/HRC/13/37, p. 1; further herein: A/HRC/13/37.

According to the UDHR and ICCPR alike the freedom from privacy intrusions ought to be enforceable through laws granting protection "against such interference or attacks".[43] When it comes to setting the limits of privacy however, there is one significant difference between the two fundamental human rights documents discussed. While the non-binding UDHR contains a general limitative clause in its Article 29 para. 2, which makes the exercise of all rights and freedoms named in the Declaration subject to limitations determined by law "solely for the purpose of securing due recognition and respect for the rights and freedoms of others and of meeting the just requirements of morality, public order and the general welfare in a democratic society", no such general reference nor one relating directly to privacy can be found in the ICCPR, although individual limitative clauses can be found for other rights, such as Article 19 para. 2 allowing for legitimate limitation of the freedom of expression.[44] While the three-steps test for freedom of expression is may be subject to criticism as extensively vague,[45] it sets the basic standards states must meet when providing human rights guarantees to individuals within their jurisdiction. This is not to signify however that the right to privacy is an absolute one. As clearly visible in other human rights treaties, just to mention Article 8 of the European Convention on Human Rights (ECHR),[46] privacy as any other human right may be subject to limitations provided for by law and necessary in a democratic society for the protection of rights and freedoms of others.

The need to outline a limitative clause for privacy was met with the series of **HRC** documents, staring in 1988 and the General Comment No. 16 mentioned above. In this elementary document the HRC clearly stated that according to the existing human right standards "Surveillance, whether electronic or otherwise, interceptions of telephonic, telegraphic and other forms of communication, wire-tapping and recording of conversations should be prohibited."[47] While this is by far not the only document wording the need to provide legitimate legal grounds for any surveillance it must be

[43] Article 12 UDHR, Article 17 ICCPR.
[44] Article 19 and its limitative clause are discussed in detail in the following subparagraph.
[45] See para. 4 herein below.
[46] Convention for the Protection of Human Rights and Fundamental Freedoms, Council of Europe, 1950, CETS 005.
[47] A/HRC/13/37, pt. 8 p. 2.

noted that already as early as 1988, before the Internet gained its commercial value,[48] the HRC provided guidance directly applicable to online communications. In its comment the HRC confirmed the applicability of the three steps test to privacy. Any invasion of privacy must be lawful and non-arbitrary, while no interference can take place „except in cases envisaged by the law",[49] while relevant legislation must specify in detail the precise circumstances in which such interferences may be permitted, and „a decision to make use of such authorized interference must be made [...] on a case-by-case basis".[50] Preventing arbitrary interference the HRC emphasized that „even interference provided for by law should be in accordance with the provisions, aims and objectives of the Covenant and reasonable in the particular circumstances".[51] The existing human rights regime obliges states not only to refrain from breaching individual human rights, including the right to privacy, but also to act in order to provide their effective protection. The HRC emphasizes this due diligence obligation when stating that „Effective measures have to be taken by States to ensure that information concerning a person's private life does not reach the hands of persons who are not authorized by law to receive, process and use it".[52]

The 1988 General Comment was followed by other UN documents dealing directly or indirectly with the limits of individual privacy perceived as a human right. While the right to privacy is under particular threat from state security operations, it is the question of its limits in counter-terrorism state actions that holds significant value. It is the 2009 Report of the UNHRC Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism that provides a

[48] In 1991 the US National Science Foundation, funding the "Internet" research project allowed for setting up of the Commercial Internet eXchange (CIX), making the up-till-then purely academic network open to commercial use. The very same year CERN introduced its "world wide web" protocol, significantly enhancing the commercial value of the network by making its operation more user friendly. See: Review of NSFNET, Office of the Inspector General, National Science Foundation, March 23, 1993, available at: http://www.nsf.gov/pubs/stis1993/oig9301/oig9301.txt.
[49] A/HRC/13/37, pt. 3, p. 1.
[50] A/HRC/13/37, pt. 8, p. 2.
[51] A/HRC/13/37, pt. 4, p. 1.
[52] A/HRC/13/37, pt. 10, p. 2-3. Due diligence in preventing human rights invasions is discussed in the following paragraph.

detailed analysis of the fragile balance between state security and individual privacy.[53] The Special Rapporteur argues that Article 17 enables for a "necessary, legitimate and proportionate restrictions to the right to privacy", while containing "elements of a permissible limitations test".[54] Based on this assessment he finds it required by international law for states to "justify why a particular aim is legitimate justification for restrictions upon article 17" and emphasizes the role new technology have had on the erosion of privacy.[55] Echoing the work of the HRC and summarizing the jurisprudence of the Optional Protocol Scheinin identifies seven criteria any privacy restriction must meet. Those include: their provision by law, non-interference with the essence of the right, necessity in a democratic society, no unfettered discretion, the necessity of any restriction to reach, rather than just aim, one of the legitimate aims, proportionality of the restrictive measures and consistency with other ICCPR-granted rights.[56]

Referring to best practice examples Scheinin proposes five principles applicable to any privacy restriction introduced in accordance with the ICCPR regime. He opts for a principle of minimal intrusiveness, encouraging states to ensure they have "exhausted the less-intrusive techniques before resorting to others."[57] Following the British example, he recommends a data-minimization principle that encourages states to "resist the tendency" to collect forever more personal data, even when not necessary, but technically possible.[58] Another proposed guideline is expressed by the principle of "purpose specification restricting secondary use", obliging states to introduce legal safeguards for using data for reasons other than those identified as grounds for their initial collection, while referring to the existing human rights framework as the tool to ensure transnational data exchange legality.[59] Another guideline for privacy respecting legislature is a principle of "oversight and regulated authorization of lawful access".[60]

---

[53] Human Rights Council, Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, Martin Scheinin, Dec. 28, 2009, A/HRC/13/37.
[54] *Id.*, p.2.
[55] *Id.*, p.1.
[56] *Id.*, para. 17.
[57] *Id.*, para. 49.
[58] *Id.*, para. 49.
[59] *Id.*, para 50.
[60] *Id.*, paras. 51-53.

This notion encourages introducing effective safeguards for the supervision of data collection and processing entities, also coming from independent reviewers. The fourth principle for privacy protection is that of "transparency and integrity" requiring openness and communication among states on their surveillance practices.[61] This principle reflects the personal data protection regulations granting individuals the right to access information about them collected by private and public bodies. Eventually, reflecting the fast-paced technological progress the Special Rapporteur recommends "effective modernization" as the fifth principle of privacy protection in the modern society. According to him the ease with which data may be collected is not reflected in the level of legislative and technological measures for securing them from unauthorized use or access. Privacy impact assessments, introduced by some states and forever more companies are recommended as a tool to fight this lack of proportionality.[62]

4.2. Freedom of expression

Just as the practical application of Article 17 requires some supplementary implementation done by the UN and its Special Rapporteurs, also Article 19 UDHR and other freedom of speech regulations have been thoroughly analyzed by UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression with particular regard to online communication.[63] As the key to applying existing standards online lies in their appropriate implementation, Special Rapporteur on the promotion and protection of the right to freedom of opinion and protection, Frank LaRue, provided detailed guidelines on such proper adoption, following previous work of the HRC and other Special Rapporteurs. With the limited scope of this paper in mind, just two of the numerous documents will be discussed, as a representation of the UN line of reasoning. In its 2011 General comment No. 34 on the freedoms of opinion and expression, laying down the interpretation of Article 19 ICCPR the HRC recognized the complementary freedoms: of opinion and of expression as indispensable conditions

[61] *Id.*, paras. 54 - 55.
[62] *Id.*, para. 57.
[63] Report of the Special Rapporteur to the General Assembly on the right to freedom of opinion and expression exercised through the Internet, 2011, A/66/290; Report of the Special Rapporteur on key trends and challenges to the right of all individuals to seek, receive and impart information and ideas of all kinds through the Internet, 2011, A/HRC/17/27.

for individual development of each human being.[64] Protection of those freedoms lies at the foundation of transparency and accountability of every democratic society.[65] While the component freedom to hold opinions may suffer no exception or restriction,[66] the abovementioned three steps test is to be applied when limitations are being put onto the freedom of expression. Details of the limitations are contained in Article 19 para. 3 ICCPR, forming the special duties and obligations resting upon those exercising that right. Two areas where certain limitations on the freedom of expression may be enforced cover: such exercise of the freedom which endangers or infringes the rights or reputation of others or, on the other hand, when such limitations are called for in order to protect public order, health or morals.[67] No limitation of this right however may endanger its very core – it may never be as extensive as to actually deprive the individual of his or her liberty to share ideas, where it is the freedom of expression that is the rule and any limitation thereof must maintain the character of an exception, not vice versa.[68] As already mentioned any limitation of the right to free expression may be exercised solely if it is 1) provided by law 2) imposed for one of the two grounds named above and 3) necessary and proportionate.[69] Any such restrictions may only be applied for the purpose for which they were introduced and applied directly to the particular need they cater for.[70] Moreover, states are under an obligation to protect individual freedom of expression from limitations affected by third parties, including private entities.[71] This obligation is of particular importance for the multilayered and multistakeholder online environment. States' positive obligation to undertake all necessary measures to protect the freedom of expression of individuals from limitations other than those provided for by law, necessary and proportionate make states the actual warrants of this particular human right. Any law providing for a restriction of the freedom of expression must be sufficiently precise as to enable an individual to foresee

[64] Human Rights Committee, General comment No. 34, Article 19: Freedoms of opinion and expression, 102nd session, July 2011, U.N. Doc. CCPR/C/GC/34, para. 2; further herein: CCPR/C/GC/34.
[65] *Id.*, para. 3.
[66] *Id.*, para. 9.
[67] *Id.*, para. 21.
[68] *Id.*, para. 21.
[69] *Id.*, para. 22.
[70] *Id.*, para. 22.
[71] *Id.*, para. 23.

the consequences of their particular conduct.[72] Moreover, any limitation provided for by law may not allow for the unfettered discretion on behalf of state authorities or any other party.[73] The obligation of states to safeguard freedom of expression within its jurisdiction includes also the reversed burden of proof for any violation of this human rights – as the HRC explains, it is for the state authorities to demonstrate that the legal basis for imposed restrictions of freedom of expressions are intact with the ICCPR.[74]

Practical application of those guiding principles becomes most controversial when confronted with the increased concern for public safety in the are of the above mentioned ongoing war on terror. Also the US massive cybersurvailance was justified in national laws as needed for the reasons of state security and protecting *ordre public*. Yet the protection of public order, foreseen in Article 19 para. 3 as one of the grounds for limiting individual freedom of expression, when applied as legislative basis for state actions, must meet all other prerequisites, remain proportionate and necessary to directly achieve a given aim. This particular interrelationship between freedom of expression and state security was emphasized by UN Special Rapporteur La Rue in the context of the NSA scandal. When introducing his 2013 report on promotion and protection of the right to freedom of opinion and expression[75] he emphasized that the freedom of expression cannot be ensured without respect to privacy in communications.[76] In the Report LaRue urges "to review national laws regulating surveillance, ensuring better protection to privacy in communication, and raise public awareness of the increasing threats to privacy posed by new communication technologies."[77] Reflecting the multistakeholder nature of Internet governance, he emphasizes the need to also hold private actors responsible for human rights violations.

---

[72] *Id.*, para. 25.
[73] *Id.*, para. 25.
[74] *Id.*, para. 27.
[75] Human Rights Council, Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue, U.N. Doc. A/HRC/23/40, further herein: A/HRC/23/40.
[76] Office of the High Commissionner on Human Rights, State communication surveillance undermines freedom of expression, warns UN expert, June 4, 2013, available at: http://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=13400&LangID=E.
[77] *Id. Id.*

He stresses that measures must be taken to prevent the commercialization of surveillance technologies across the globe and the protection of communication data.[78] Upon emphasizing the interrelationship between the right to privacy and freedom of expression[79] LaRue reiterates the permissible limitations to both rights, based on the three steps test described above.[80] When discussing the vast array of technologies at hand of states exercising online surveillance, he identifies five basic tools for monitoring online activities and, consequently, limiting free expression of Internet users, which include:[81] 1) targeted communications surveillance, 2) mass communications surveillance 3) access to communications data 4) Internet filtering and censorship and 5) restrictions on the right to anonymity. Despite the detailed UN guidelines on both: privacy and freedom of expression, state practice raises significant concerns over 1) lack of judicial oversight[82] 2) too vast and too numerous exceptions to free speech guarantees in national security laws[83]; 3) unregulated access to communications data[84] 4) extra-legal surveillance[85] as well as 5) extra-territorial application of surveillance laws;[86] 6) mandatory retention of telecommunications data;[87] 7) identity disclosure laws[88] as well as 8) legal and practical restrictions on the use of encryption accompanied by key disclosure laws.[89] When repeating the principles of freedom of expression protection identified by the HRC vis-à-vis states, LaRue goes a step further and emphasizes the role and responsibilities of the private sector in respecting human rights online.[90] When noting that it is the private sector who have "been complicit" in developing mass or invasive surveillance technologies "in contravention of existing legal standards" he stresses states' failure to regulate this area of free market.[91] Reflecting the observations presented hereinabove, he emphasizes states positive obligations to "not only respect

[78] *Id. Id.*
[79] A/HRC/23/40, paras. 19-23.
[80] *Id.*, paras. 28-29.
[81] *Id.*, paras. 33 – 49.
[82] *Id.*, paras. 54 – 57.
[83] *Id.*, paras 58 – 60.
[84] *Id.*, para. 61.
[85] *Id.*, paras. 62 – 63.
[86] *Id.*, para. 64.
[87] *Id.*, paras. 65 – 67.
[88] *Id.*, paras. 68 – 70.
[89] *Id.*, para. 71.
[90] *Id.*, paras. 72-77.
[91] *Id.*, para. 75.

and promote the rights to freedom of expression and privacy, but protect individuals from violations of human rights perpetrated by corporate actors".[92] Referring to the due diligence standard present in international law, LaRue clearly states that national authorities "should exercise adequate oversight in order to meet their international human rights obligations when they contract with, or legislate for, corporate actors" whose action shape the scope and enforcement of human rights.[93] Special Rapporteur clearly states that they "must ensure that the private sector is able to carry out its functions independently in a manner that promotes individuals' human rights", disallowing "corporate actors (…) to participate in activities that infringe upon human rights".[94] States are under a direct human rights obligation to "hold companies accountable" for any direct or consecutive human rights violations.[95]

In order to achieve an effective human rights protection framework for the online environment, LaRue recommends updating and strengthening national laws and legal standards dealing with the freedom of expression,[96] giving Internet users the tools to effectively protect themselves by facilitating private, secure and anonymous communications;[97] raising human rights awareness among Internet users;[98] state regulation of the commercialization of surveillance technology[99] as well as introducing an up-to-date re- assessment of international human rights obligations resting upon all parties.[100]

All those recommendations mirror those provided by the Special Rapporteur on privacy and terrorism, Scheinin, discussed above. It seems that the theoretical background for the "appropriate" introduction of human rights standards in the online environment has strong foundations. The work of Special Rapporteurs Scheinin and LaRue allowed the UNHRC to officially recognize human rights online applicability in its 2012 Resolution

[92] *Id.*, para. 76.
[93] *Id.*, para. 76.
[94] *Id.*, para. 77.
[95] *Id.*, para. 77.
[96] *Id.*, paras. 81-87.
[97] *Id.*, paras. 88-90.
[98] *Id.*, paras. 91-94.
[99] *Id.*, paras. 95-97.
[100] *Id.*, paras. 98-99.

on promotion, protection and enjoyment of human rights on the Internet.[101] Although filled with diplomatic emphasis, which might be considered a modest, legally cryptic political text it is the first international document to recognize the need of re-adaptation of the existing human rights catalogue to the online environment and new technologies. The preceding documents, discussed briefly above, allow to identify the road ahead for the development of human rights obligations in the information society, ones applicable not only to states but also to private actors.

4.3. The significance of the 2012 UN Resolution

The brief resolution, consisting of 5 paragraphs, expresses the essential applicability of human rights jurisprudence to online communications. Adopted by 71 parties,[102] including states known for their filtering and surveillance policies like the United States, Turkey, India, Egypt and Tunisia, the Resolution directly "affirms that the same rights that people have offline must also be protected online" with particular emphasis to online freedom of expression, according to the existing article 19 UDHR standards. Reflecting the WSIS Tunis Agenda it makes a reference to the "global and open nature of the Internet as a driving force" for progress and encourages states to "promote and facilitate" Internet access.[103]

It seems that the UN is on its way to undertake the challenge of resolving the human rights online issue. It must be emphasized however, that as much as the applicability of global, yet locally interpreted human rights may be considered a difficult challenge for the global information society, it is the diplomatic will that is determinant of any success in their effective protection. Regarding the existing detailed UN guidelines on privacy named above and the recent NSA controversy, which deployed massive surveillance without legitimate aim and case-asserted validation, it is not the legal challenge but the political motivation that is decisive for effective human rights protection online.

[101] UN Human Rigths Council Resolution on promotion, protection and enjoyment of human rights on the Internet, June 2012, UN Doc. A/HRC/20/L.13, further herein: A/HRC/20/L.13.
[102] The support of a little over 1/3 of the UN member states reflects perfectly the fraction of Internet users among the world's population, see supra 4 above.
[103] A/HRC/20/L.13, para. 3.

5. A question of due diligence

While awaiting further UN action aimed at facilitating effective human rights protection online one remark must be made. According to existing human rights treaties states have a both: a negative but also a positive obligation to strive for effective protection of individual human rights for those within their jurisdiction. As with any international obligation of conduct, the assessment of state actions and omission will rest upon a due diligence standard. Due diligence requires states to take up "all reasonable measures" in order to meet their international obligations, while a failure to do so may result in their international responsibility.[104]

According to the extensive studies of the International Law Commission (ILC), summarized within two key documents: the 2001 ILC Draft Articles on Responsibility of States for Internationally Wrongful Acts[105] and the 2006 Draft Principles on the Allocation of Loss in the case of Transboundary Harm Arising out of Hazardous Activities respectively[106] a due diligence principle accompanies any obligation of conduct and consists of nine elements. Due diligence requires states to act in good faith when meeting their international obligations, including any preventive duties. Secondly, it is closely related to the principle of good neighborliness, requiring states to refrain from causing harm or damage within the territory or in the interests of other states as well as in common territories. Due diligence assessment ought to be conducted with respect to state territory and it is potentially harmful actions initiated within state territory that must be prevented. Fourthly due diligence obligation is a derivative of the principle of sustainable development, as due diligence should also accompany the risk assessment of introducing any new procedure or legislation. The fifth element of the due diligence principle is a state's obligation to undertake "all necessary measures" expected of a "good government" in order to meet the goal of an obligation, while the particular

[104] See: Ricardo Pisillo-Mazzeschi, *The "Due Diligence" Rule and the Nature of the International Responsibility of States,* 35 German Yearbook of International Law 9 (1992), at 9 – 49.
[105] Draft Articles on State Responsibility: Titles and texts of articles adopted by the Drafting Committee, International Law Commission, UN Doc. A/CN.4/L.472; (2001) II (2) Yearbook of the International Law Commission 31 ff.
[106] (2006) II (2) Yearbook of the International Law Commission 101 ff., UN Doc. A/61/10. The obligations of prevention were expressed within the 2001 ILC Draft Articles on Prevention of Transboundary Harm from Hazardous Activities, (2001) II(2) Yearbook Of The International Law Commission at 144.

content of such an obligation is always case-specific. Those particular measures will strongly depend on the state of art in a given area set against the economic and technological capabilities of a state. Consequently the seventh element of due diligence is an obligation to exchange information with international counterparts regarding the risks assessed and measures taken for preventing a breach of international obligations. According to the work of ILC states are also obliged to refrain from any discrimination of either victims of a certain breach or their originators. Eventually the due diligence standard is one of continuous nature, obliging states to upkeep their efforts in assessing and preventing breaches of their international obligations.[107]

In this context it may be assessed that states hold a due diligence obligation in preventing breaches to individual human rights. In order to meet that obligation they ought to engage in international cooperation and actively seek to undertake "all necessary measures" to prevent human rights violations within their jurisdiction, power or control. This does not mean that they are obliged to successfully prevent any breach or to have knowledge of any attempt of such violation. They are to deploy actions expected of a good government in a given situation. While a state is therefore not obliged to undertake particular measures to e.g. make sure content originating from its territory is available elsewhere, guaranteeing the fulfillment of an individual right to communicate, it should act when informed of surveillance of its residence by foreign powers, aiming for such violations of individual's rights to cease. Human rights protection online is therefore a two sided concept, including on one hand an obligation to refrain from interference with an individual human right, yet at the same time – to undertake in due diligence all necessary measures aimed at preventing any such breach affected by a third party within state jurisdiction.

As with any international obligation, the lack of due diligence on behalf of state authorities in actively undertaking measures to prevent breaches of privacy, freedom of expression or any other individual right might result is state responsibility according to

[107] For an extensive analysis of the due diligence principle in international law see generally: Joanna Kulesza, Należyta staranność w prawie międzynarodowym [Due Diligence In International Law] (2013).

the rules identified in international law when no circumstances precluding lawfulness would arise, such as necessity or force majeure.[108]

6. Summary

Although applying human rights online may seem a challenge, existing international law provides detailed guidelines for their enforcement in cyberspace. Rich human rights jurisprudence and scholarly writing allow to identify the limits of allowed intrusions of individual rights, while international law on state responsibility contains states' obligation to actively prevent breaches of human rights within their jurisdictions. It seems therefore that the HRC 2012 Resolution of human rights applicability online is the first step towards applying the rich human rights law to the online environment, following the recommendations and analysis provided by UN Special Rapporteurs as well as academia and civil society, reiterated above. The crucial element for the successful human rights protection is therefore not the legal challenge but rather the lack of political will. Such political will may be provoked by the civil society, aware of its rights and states' obligations. As examples of the Arab Spring or the ACTA demonstrations showed, the cyberspace is an effective tool for increasing society participation and raising individual awareness. As Internet users become more aware of their rights, states are bound to be made more aware of their human rights obligations, including their duty to hold private corporations accountable for their involvement in human rights violations through e.g. exporting surveillance technologies.

The Internet revolution has inflicted one significant change on the public and international law landscape – the increased role of soft law, seen as non-enforceable guidelines shaping future polices. Due to its multifaceted character and complexity, it is difficult to position the Internet under any single international legal regime; thus, most contemporary international documents relating to Internet governance are deemed to be of a soft law nature. Yet this distinction is challenging due to the ambiguous nature of

[108] See the discussion on interdependence between state responsibility and international liability in the works of Dupuy, i.e. Pierre Dupuy, *Dionisio Anzillotti and the Law of International Responsibility of States*, 3 EJIL 139, (1992), at 139 – 148; Pierre Dupuy, *The International Law of State Responsibility: Revolution or Evolution*, 11 Michigan Journal of International Law 105 (1989) at 105 – 128.

the division between hard and soft law.[109] McDougal and Lichtenstein question the very distinction between law and policy,[110] while Fastenrath finds soft law crucial in terms of exercising any political impact.[111] In the context of states' international obligations, the generally acknowledged distinction between hard and soft law lies in the possibility of being able to hold states responsible for failing to meet such obligations. While a state that breaches an obligation specified within a treaty or customary law practice may be held internationally responsible for doing so, no legal consequences may be laid upon it for failing to meet a soft law requirement, enshrined, for example, within a declaration or a recommendation of an international organisation or an expert group. Such documents may be considered additional sources for identifying an existing customary norm, yet they need to be accompanied by uniform state practice and judicial decisions confirming the binding character of norms enshrined therein. However, this seemingly simple theoretical distinction between hard and soft law, identifying individual obligations as originating from a treaty or universal or regional customary law proves itself to be most difficult in practice in all areas of international relations, and in particular when it comes to holding parties responsible for human rights violations.[112] Therefore it is primarily soft law documents, such as the 2012 UNHRC Resolution on promotion, protection and enjoyment of human rights on the Internet accompanied by other documents discussed hereinabove that are bound to shape future policy making, both nationally and on the international arena.

[109] The significance of this issue is highly visible in the vigorous debate between distinguished international law scholars dating back to 1988 when a consensus on the very definition of soft law is hard to find: Antonio Cassese, Joseph. H. H. Weiler (eds), Change and Stability in International Law-Making (1988) at 77–90.
[110] Myres Smith McDougal, *International Law, Power and Policy: A Contemporary Conception,* 82 Recueil des Cours 1 (1954), at 133; Cynthia Crawford Lichtenstein, *Hard Law v. Soft Law: Unnecessary Dichotomy?*, 35 The International Lawyer 1421 (2001), at 1433.
[111] Ulrich Fastenrath, *Relative Normativity in International Law*, 4 EJIL 301 (1993), at 305.
[112] *See*: the sources cited above.