**WORKING PAPER**

THE NETHERLANDS INSTITUTE OF HUMAN RIGHTS (SIM)
UTRECHT UNIVERSITY, THE NETHERLANDS

# PUBLIC PRIVACY
# HUMAN RIGHTS IN CYBERSPACE

BY

ANJA MIHR
ASSOCIATE PROFESSOR

16 DECEMBER 2013

UTRECHT, THE NETHERLANDS
EMAIL: A.MIHR@UU.NL
WWW.ANJAMIHR.COM

# PUBLIC PRIVACY: HUMAN RIGHTS IN CYBERSPACE[1]

## INTRODUCTION

Public Privacy is about basic freedom and privacy rights grounded in international human rights law. Cyberspace is a borderless public space in which citizens, regardless of their citizenship, nationality, ethnicity, political orientation, gender or otherwise background communicate and interact. Through new technologies, Cyberspace offers an environment that consists of many participants with the ability to affect and influence each other. This space is transparent and neutral in its nature but often defined, broadened, limited and censored by people who make use of it. Communication via the internet is therefore often anonymous and yet used and shared with a worldwide wide public, which remains, to the large part, personally unknown for the individual internet user, namely us. Nevertheless, we do share some of our most private and personal data with this anonymous audience. This worldwide public counts today around 2.5 billion internet users. If cyberspace were a country, it would be the largest and most populated country in the world, but yet without any government, legislative bodies, law enforcement, protection mechanism, or rules for participation, let alone anything that comes close to a 'cyber-constitution' for all internet-citizens. We assume that without a commonly accepted 'cyber-constitution' based on human rights and the rule of law based on effective measures and mechanisms to enforce these rules, the internet-citizens or citizens 2.0 of this world will have difficulties to protect and enjoy their human rights in cyberspace.

By sharing private information, billions of internet users have already created virtual twins in this new space, without ever having a chance to delete information. Personal relationships and 'being friends' through social networks such as Renren and Facebook can be anonymous on the one side, and yet provide a vast amount of personal data and private messages. People's private as well as professional lives are publically moving in cyberspace. Businesses and enterprises, education and training, finances and economics, private correspondence, and even health and personal issues are now

[1] Special thanks to Jessica Porta and Jorge Rodriguez Rodriguez for their editorial support. Gratitude to Ellen Wesselingh for her helpful comments.

dealt with by anyone who seeks access to it in this ‘endless’ space.[2] The vehicle by which information moves in this space is the internet and it moves on the highway called World Wide Web. But seemingly to national space and territory that we call a country or a state, the way people and actors behave and make decisions in this space is guided through principles and norms usually written down in constitutions or laws. Ideally these rules, regulations and laws are set up by the citizens for the citizens. That process of setting up common and joint rules and standards by internet-users for internet-users has not taken properly place in cyberspace, yet. Most of its mechanism so far have been ill-suited. Nevertheless, the normative legal and political framework that we find within state borders could also be transferred to the cyberspace, because it is defined by universal values and norms, such as the international human rights norms and rules. Ultimately, what is missing in cyberspace is a quasi-government or governance regime that governs the needs and claims of its citizens through monitoring and enforcement bodies. In the case of Cyberspace, these citizens are internet users all around the world. Although international governmental organizations (IGOs), such as the UN, the Organization for American States, the African Union or the European Union, aim to set international standards for the use of cyberspace and internet to be respected and enforced by national governments, they generally fail to do so. The reason for this is that states’ powers and enforcement mechanisms often end at state borders because their mandate to protect human rights is entirely based on state sovereignty and governments. IGOs and international courts often also have only limited measures and means to protect human rights, let alone enforce them.

Because cyberspace has no physical or national borders, the means and ways to govern this new borderless regime are not yet defined. Nevertheless, in the debate and effort to set up a cyberspace governance regime, human rights norms and standards (such as the human rights to privacy, security, health, free expression, movement and enterprise) give guidance to the various number of different actors that are involved in the design of the cyberspace regime and how to possibly regulate it. If ever established, the cyberspace governing body will be one of multiple stakeholders and actors including national, international as well as private actors, such as representatives of companies, social networks, NGOs and individuals.

[2] Mindaugas Kiskis (2011) Entrepreneurship in Cyberspace: What do we know?, Social Technologies, Mykolas Romeris University, 1 (1), 37-48. http://www.doaj.org/doaj?func=fulltext&aId=1045782 (Access December 2013).

## PUBLIC PRIVACY

Public Privacy is a notion that encompasses the respect for human rights and fundamental freedoms fostering in the protection of our data, security, and privacy in the cyberspace. It is the freedom of information and expression in the internet on the one side, and security and privacy on the other side in the cyberspace. According to international standards and definitions, privacy is a private and personal space in which we develop our personality in a confident and free way and exercise our skills and capacities, maintain our health and enjoy social relationships with family and friends.[3] Hence, privacy in the cyberspace means using the internet as a service tool for private purposes without fearing that third parties, such as governments or companies (i.e. national security agencies, Google+ or Microsoft) are accessing, selling or publically posting our data for security or business purposes without our consent.

The right to freedom is stated in various international treaties and agreements. It encompasses the right of free expression, which includes the freedom to hold opinions and to receive and impart information and ideas without State interference. This right also includes the right to communicate and to express oneself in any medium, including through words, pictures, images and actions including exchanging ideas and thoughts through social networks or other internet platforms, to protest against misconduct and to demonstrate. Freedom means the right to political expression including comments on matters of general public interest; artistic expression; and commercial expression, particularly when it also raises matters of legitimate public debate and concern. Because most democratic countries foster the installment of internet for market economy reasons and better communication, political expression is given particular precedence and protection. To ensure that free expression and debate is possible, there must be protection for elements of a free internet and media such as printed and online press, including protection of journalistic or investigative sources.

Eventually, the challenge Public Privacy is facing is how to balance our personal, professional and private interests using the internet as a free and open access communication tool and benchmark our actions and rules against privacy and freedom rights for all.

The debates and discussions around freedom and privacy rights in the internet are of fundamental importance under the notions of data protection, cybersecurity, cybersurveillance or cyberwar through cyberviruses. Some already call it the World Wide War in which various actors, such

[3] Helen Nissenbaum, ‘Toward an Approach to Privacy in Public: Challenges of Information Technology (1997) 7 (3), *Ethics & Behavior*, 207-219. http://www.nyu.edu/projects/nissenbaum/papers/toward_an_approach.pdf

as states and non-state actors, such as hackers, are equally involved. Commercial state or inter-governmental agreements like SOPA, PRISM, PIPA or ACTA are just a few international governmental initiatives to regain the control over the borderless dataflow. They aim to control the access to data. Although some governments attain to protect our data in the internet, these inter-governmental agreements can lead to massive misuse and abuse of private data that can affect many others fundamental freedoms and basic human rights. The challenge will be to assess how human rights can be fully guaranteed under these arrangements and agreements. The complete absence of effective data protection will have repercussions and consequences both in leveraging human right realization and in preventing people from enjoying human rights.

## HUMAN RIGHTS IN CYBERSPACE

To mention but a few fundamental freedoms and privacy human rights that are dealt with in this context are, for example, free expression of belief, political opinion, art and written texts; the free and equal access to information; and the protection of privacy issues such as family relations, friendships or health issues. Furthermore, human rights in cyberspace is about the protection and security to be free from harassment and persecution on internet for a based on one's own political, ethical or gender identity as well for hers or his private professional, educational or health data without his or her consent. It is about protecting one's own intellectual property and creativity, i.e. art, movies, pictures, literature, scientific results, as well as having access at any time to fair and open trials – to name but a few.

The often proclaimed "Right to Internet" which aims to allow individuals have access to internet at any time and the "Right to be Forgotten" which assures that one's own private data remains private and can be deleted at any time, are already part of the overall human rights standards concerning access to information, the right to privacy and data protection (as in the EU Fundamental Rights Charta) and participation. Yet, how to realize these rights and turn them into active legislation has to be seen. Case law will most likely take quite some time to establish interpretations of these rights, although the Research Division of the European Court of Human Rights has already in 2011 published a groundbreaking documents on the potential the Case-law concerning data protection and retention issues relevant for the internet could mean in future decisions taken by the court. In this document the freedom of expression, intellectual property and issues of cybercrime are seen the major deficits that yet have to be further defined and interpreted through case law.[4] Further below, I will give two examples of recent cases ruled by the court in 2012 and 2013 under these provisions.

The fact that basic human rights principles and norms are universal has been reconfirmed in 1993 during the World Conference for Human Rights in Vienna, Austria.[5] It is therefore no longer an issue of international debates whether freedom rights exist or not, but rather how to implement and enforce them into national legislation. During the conference, all UN member states confirmed that all human rights derive from the dignity and worth inherent in the human person, and that the human person is the central subject of human rights and fundamental freedoms, and consequently should be the principal beneficiary and should participate actively in the realization of these rights and freedoms.[6] According to this statement, human rights are rights inherent to all human beings, regardless of nationality, place of residence, sex, national or ethnic origin, color, religion, language, or any other status. We are equally entitled to the protection and promotion of these human rights without discrimination. They are interrelated, interdependent and indivisible. Human rights embrace sets of different values such as solidarity, confidentiality, fairness or friendship as well as principles, norms and standards such as the right to fair trial, the freedom of expression, or the right to adequate housing, access to water or access to information. Human rights are often written down and guaranteed by law treaties, customary international law, general principles and other sources of international law.[7] They include obligations and duties of governments, companies, individuals or other legal entities (duty-bearers) to act in certain ways or to refrain from certain acts. Duty-bearers, such as governments, have to protect the human rights of right-holders, that is to say any person and citizen on this planet, regardless of his or her background. Human rights are often named as social, civil, economic, policical or cultural and there is no hierarchy between them. Social human rights are, for example, the right to education, health, social security, family and marriage. Civil rights are those to participate, to assemble, to live in dignity, to enjoy fair and open trial, to be free from torture, and to enjoy physical integrity. Economic human rights are those to work, to adequate salary, to enjoy holidays, and to set up enterprises. Political rights are those to vote or be elected, to participate in decision making processes, and so on. Cultural rights are those to religious freedom and practice, as well as customs and traditions.

[4] Council of Europe, ECtHR, Research Division (2011) ‘Internet: Case-law of the European Court of Human Rights, Strasbourg, June 2011 www.echr.coe.int. (Access December 2013).

[5] UN Doc, GA A/CONF.157/24 (Part I), Report of the World Conference on Human Rights by the UN Secretary-General, October 1993 http://www.unhchr.ch/Huridocda/Huridoca.nsf/(Symbol)/A.CONF.157.24+(Part+I).En (Access December 2013)

[6] World Conference on Human Rights, 14-25 June 1993, Vienna, Austria.

[7] UN Doc. General Assembly Resolution 217 A (III). Preamble of the Universal Declaration of Human Rights. 18 December 1948.

Eventually, all these different categories of human rights cannot be exercised or enjoyed without one another. The right to housing or to work, the freedom of religion or the right to health can only be enjoyed or pressed for if the human rights to assemble, protest and participate allows us to make open claims for these rights, in case they are not executed or respected. This is the holistic approach to human rights under the principle of the so called Golden Rule of 'do no harm to others as you would have them to do to you'.[8] This means, that all these human rights ought to be balanced and estimated insofar as they do no harm the rights of others.

The human right to information, for example, applies to the extent that this information does not violate the dignity or privacy of others. For example, if very personal information about health or family would be accessible for everyone, it carries the risk that this information violates the rights of the person concerned. Yet, protection of data should never justify censorship or random surveillance. It is here where the balance starts and it depends very much on who decides about the limits and borders of freedom to information. The more stakeholders involved, the more likely this balance and result might be accepted by most people.

For example, the right to enjoy scientific progress under the International Covenant on Economic, Social and Cultural Rights (ICESCR)[9] from 1966 specifies in Art 15 that 'everyone enjoys the benefits of scientific progress and its applications' on, for example, scientific research and medicine patents or copyrights on technology and art. These rights are valid offline as well as online, and it makes therefore no difference whether we illegally copy an artefact in a museum or in cyberspace; both acts are a violation of human rights. In Art 13, for example, the human right to education is mentioned. It means that education should be made accessible, offline as well as online, to train, educate and empower people in order to develop their human personality. They should be empowered to participate in decision making processes in their professional lives and to govern societies. This right also includes access to online teaching or to E-Governance. Art 17 of the UN International Covenant on Civil and Political Rights (ICCPR) from 1966 states that no one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, or to unlawful attacks on his honor and reputation. This article is fundamental for the understanding of the protection of our freedom and privacy rights in cyberspace, because in this article we read further that everyone has the right to the protection of the law against such interference or attacks. Most liberty and freedom rights are found in this covenant as well as in other international human rights treaties in

[8] Internet Encyclopedia of Philosophy, The Golden Rule, 2010 http://www.iep.utm.edu/goldrule/ (Access December 2013)

[9] These human rights are expressed in mayor international treaties, such as the ICCPR and the ICESCR 1966.

Africa, Europe, the Arab World or the Americas; for example, Art 3 establishes the non-discrimination principle, Art 18 mandates freedom of religion, Art 19 upholds the freedom of expression, Art 20 mandates sanctions against inciting hatred and Articles 21 and 22 mandate freedom of association, and so on.

All these human rights, to name but a few, are internationally recognized and even though some countries have not ratified these covenants, most of these rights have turned into customary international human rights law. This means that even if countries have not ratified certain international treaties, these human rights are generally valid and applicable, i.e. within national jurisdiction. They are customary and general, because the majority of people around the world aheres to them or includes aspects of them in their national legislation or legal procedures. Ultimately, they are all valid both online and offline and there is no difference whether they are violated in cyberspace or within physical space and borders. Yet, the open question remains: who can protect, implement and enforce human rights in cyberspace, if governmental mandates end at their state borders?

Following the controversies on cybersecurity, national sovereignty, and individual freedoms of users over the past decades, in 2011, the UN Special Rapporteur on Freedom of Expression, Frank de la Rue from Guatemala, urged governments not to cut off users from Internet access, regardless of the justification provided, including on the grounds of violating intellectual property rights law, to be disproportionate and thus a violation of article 19, paragraph 3, of the ICCPR. He called upon all states to ensure that internet access is maintained at all times, including during times of political unrest.[10] And in 2012, the UN Human Rights Council in Geneva stated that the same rights that people have offline must also be protected online and calls upon its member states to ensure freedom of expression and the access to internet, or, for example, the access to international cooperations that provide media information such as social networks, search engines, etc.[11]

In 2013, during a number of occasions and events on the international and national level, such as the NSA affair between the USA, Germany or Brazil, the issues of cyber espionage and misuse of private data came about. In consequence and response to these different developments and incidents, the UN Special Rapporteur de la Rue once again urged the UN member states to ensure that individuals are able to freely seek and receive information or express themselves whilst respecting, protecting and promoting their right to privacy. He highlighted the fact that privacy and freedom of

[10] UN Doc. A/HRC/17/27. Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue, 16 May 2011, para.23, 79.

[11] UN Doc. Doc. A/HRC/20/L.13. Human Rights Council, “The promotion, protection and enjoyment of human rights on the Internet”, 29 June 2012, para.1.

expression are interlinked and mutually dependent and therefore without adequate legislation and legal standards to ensure the privacy, security and anonymity of communications, journalists, human rights defenders and whistleblowers, cannot be assured that their communications will not be subject to states' security.[12] The UN report received many responses, in particular by the civil society organization (CSO) network community. CSOs have long claimed that human rights are not protected well enough in cyberspace. The Electronic Frontier Foundation (EFF), for example, claimed that technologies can open a Pandora's box of previously unimaginable state surveillance intrusions and metadata can reveal sensitive information that can be easily accessed, stored, mined and exploited.[13]

Hence, so far there is no regional or international human rights regime such as UN, ASEAN, EU, OSCE, OAS or AU, ready to deal with the consequences and effects of global flow of data, intellectual property, secret information or private data, even though all these regimes have the topic on their agendas. Although citizens that use internet within the borders of regional organizations such as the EU enjoy some protection, these measures are not valid globally. The USA or China have long urged for joint binding agreements to deal with the borderless data flow in order to either protect or to restrict it. In technical terms that is a fight with windmills that cannot be won by state institutions nor by international inter-governmental regimes alone. The reason why it takes more than just a few governments in international regimes, such as the UN to solve the problems is that it takes effective institutions to enforce common rules. Without the wider cybercommunity, like technical companies, internet providers, or search engines and so on, effective enforcement mechanism will less likely be established. Because the cyberspace is not restricted to states or to any geographical or physical borders, it is thus not bound to any state or inter-state agreement and not to be controlled by state institutions alone.

The international human rights regime, for example, is entirely based on states' (often non-binding) willingness and capacity to promote and protect human rights and is therefore a valid but weak institutional set up to govern cyberspace. Moreover, because this international regime depends on the joint agreements and regulations set by governments, including democratic and non-democratic ones, such as Russia, USA, Germany or China, the results are often compromises that lack of strong monitoring and enforcement mechanisms based on international human rights law. More so, other

[12] UN Doc. A/HRC/23/40. Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue, 17 April 2013, para.79.

[13] Electronic Frontier Foundation, 'Internet Surveillance and Free Speech: the United Nations Makes the Connection' 4 June 2013. https://www.eff.org/deeplinks/2013/06/internet-and-surveillance-UN-makes-the-connection (Access December 2013).

stakeholders are often excluded from this process, i.e. internet providers, let alone the global network community or the billions of individual users, namely us. The International Internet Governance Forum (IGF), one of the main forums to tackle these issues, is yet also based on national institutions andtheir agencies and delegates. It is not truly transnational, although it aims to solve transnational violations of human rights and privacy.

Still, there is no international cyber law to combat cyber-attacks or the dissemination of private data and secret files. And if this culminates into a so called cyber-war, there has to be one party that declares the war to another party. Who are these parties? A state government against whom? And as every war ends, among which parties will there be a "peace contract" if no government or sovereign agent is involved and the combatants hide behind anonymous masks? Therefore, governmental rhetoric about leaks in the cyberworld often use organic terms, such as cyber-attack, i.e. by virus, infections etc., which suggests that the Internet is "alive" and therefore requires preventive, defensive measures, similar to global diseases and threat to health. But in the case of cyberwar, the 'enemy' is the individual internet users, who 'abuse common rules' of good conduct. Nonetheless, state governments, such as the US or British government have reacted in and often irrationally and precipitant way to the threat. This was demonstrated by the scandal around PRISM and the whistleblower, Edward Snowden, in 2013 or as the consequence of secret files leaked by WikiLeaks. None of these cases seems to be resolved, let alone in a way that would mean more data protection, privacy and freedom for all internet users on a global level. The often overhasty reactions by government, when governmental or secret data files get leaked shows the shortcomings of the current legislative bodies that are in place domestically and internationally. Interestingly enough, during these scandals, confidential secret service data has been made public by individual agents that, in return, are made responsible for 'espionage' against states – an antagonism which exemplifies the lack of definition and clarification in these aspects.

Yet, efforts to 'tame' cyberspace and to give it overall rules and regulations to which we should all adhere to, is as old as the cyberspace and internet itself. In 1996, Jon Perry Barlow published the 'Declaration of Independence of Cyberspace'. In this declaration he indicated the situations and controversies that today's internet users worldwide are worried about.[14] The Declaration sets out, in sixteen short paragraphs, a rebuttal to government of the Internet by any outside force, specifically state governments. He argues that no government has yet the consent of the internet users to apply arbitrary

[14] John Perry Barlow, 'A Declaration of the Independence of Cyberspace' 8 February 1996. https://projects.eff.org/~barlow/Declaration-Final.html (Access December 2013).

laws and restrictions to the internet, and if they try to do so, as with the data protection laws within the EU or USA or the various inter-state agreements, servers will be changed and data will continue to be published through whistleblowers, hackers and “leakers” without the owner’s consent. The internet is a world outside any country's borders. Barlow assured, twenty years ago, that the Internet community and thus the global user community has to develop its own social contracts to determine how to handle its problems based on the Golden Rule, which again is also the foundation for realizing human rights. The rule can be interpreted in such a way that if one does not want to have its own private data, pictures, letters, images or intellectual property and ideas to be publically disposed without one’s consent, then one should also not dare to publish someone else’s data without that person’s consent. Whether such social contract for the cyberspace will ever be realized or not, the idea behind that is individual responsibility and adherence to human rights, which the global community, us, has long agreed to. Another protagonist who aims to set common rules for the internet is Jeff Jarvis. He came up with another claim for internet freedoms and manifested that every citizen of this world needs to enjoy the right to connect, to speak freely, to assemble and to enjoy his or her privacy. Eventually, this can only be guaranteed with open and free access to public information and public good/spheres through internet.[15]

The need for basic human rights is not disputed in this world anymore, not among cultures or among nations. Everybody agrees that freedom, justice, privacy and security are important. However, among the 2.5 billion internet users, not everyone will have the same ideas about their realization and implementation in cyberspace. Thus, there is the claim that according to these general freedom principles and norms, a social contract for cyberspace could be established. This contract would need to be enforced by all internet users, regardless whether they are private or public, companies or governments and so on. This cyber human rights regime would be based on individual responsibility and behavior and on personal disguise and sanctions against those who violate these norms. Needless to say, companies’ business practices and government relationships can result in abuses of the human rights of freedom of expression, development, health, assembly, and privacy. These human rights are often called ‘Digital Rights’ if they are exercised within cyberspace or through internet. Digital Rights, are embedded in freedom rights such as those stated in the UDHR or the ICCPRS that allow the access

[15] Jeff Jarvis ‘A Bill of Rights in Cyberspace’, 27 March 2010, http://buzzmachine.com/2010/03/27/a-bill-of-rights-in-cyberspace/ (Access December 2013)

and use of ICTs such as computers and digital media, i.e. to information, to work, to communication, to health, to participation, to expression, to development (SDGs), to assemble, etc.[16]

On 10 December 2013, the International Human Rights Day, and 65 years after the UDHR was proclaimed by the UN in 1948 over 500 writers and Noble Prize Winners from over 81 countries have signed an open petition urging the UN to draft an international bill on digital rights. They argue that the dramatic increase of spyware on private data is undermining democracy online and offline and makes human rights null and void and privacy an illusion, so they fear.[17] Reactions to their open call were internationally perceived and the petition comes at a time during which different UN bodies are working on better digital rights protection. The massive support from the user community to develop such a concept is expected to have some impact on the progress of global protection mechanism and an international binding document.

## CYPERSECURITY

Internet and the World Wide Web is not per se a safe place to put private data, but it has the potential to be so if it becomes a neutral provider of data communication. That is to say, it is a means to communicate, but it is not a guaranteed safe haven for data to be protected or privacy to be realized. Cyberspace is not an actor and therefore it cannot guarantee our freedom. Nevertheless, it is a tool to exercise our freedom rights. WE have to be aware that in this state of ‘post privacy’, as some call it, we live in a world in which everyone of us has a long data trail somewhere in the internet and cyberspace that allows for retroactive actions by anyone at any time on a global scale, by national security agencies and local authorities, by providers or by ourselves.[18]

Cybersecurity is therefore another type of security, but not another form of security. There are many types of security. Human security, for example, is a people-centered view of security that is necessary for national, regional and global stability. It is about securing "freedom from want" and

[16] Office of the High Commissioner for Human Rights, *Human Rights Indicators: A Guide to Measurement and Implementation* (Geneva: 2013) https://unp.un.org/Details.aspx?pid=23745 (Access December 2013); For the definition of digital rights see: Business and Human Rights Resource Center, ‘Ranking Digital Rights project’ : http://www.business-humanrights.org/Documents/Ranking_Digital_Rights (Access December 2013).

[17] The Guardian, *International bill of digital rights: call from 500 writers around the world (*10 December 2013) http://www.theguardian.com/world/2013/dec/10/international-bill-digital-rights-petition-text (Access December 2013).

[18] Jacob Appelbaum, ‘Elevate Open Everything’ in *Elevate Festival Opening Speech*, 25 October 2013. http://2013.elevate.at/festival/ueber-das-festival/newsmagazin/detail/news/jacob-appelbaum-elevate-open-everything/ (Access December 2013).

"freedom from fear" for all persons and therefore to assure human rights for all as the best path to tackle the problem of global or local insecurity.[19] Political security is concerned with whether people live in a society that honors their fundamental freedoms. This level of security is more likely to be achieved if internet users can participate in decision making and legislative processes of their country according to international human rights law standards, and if these laws later are complied with, for example, the Rule of Law in any country or in cyberspace.[20] Yet, Cybersecurity is the collection of tools, policies, the different security concepts, security safeguards, guidelines, risk management approaches, actions, trainings, best practices, assurance and technologies that can be used to protect the cyber environment and users' assets at any time at any place in this wide space. This includes, for example, connecting computing devices, personnel, infrastructure, applications, services, telecommunications systems, and the totality of transmitted and/or stored information in the cyber environment. Cybersecurity, therefore, strives to ensure the attainment and maintenance of the security properties of users' assets, data and information against relevant security risks in the cyber environment. The general security objectives are comprised of the integrity of information and data authenticity and non-repudiation, and aim to secure data in a confidential manner.[21]

In an essay on the Critical Theory of Cyberspace, Michael Froomkin highlights that the internet is a neutral tool that can improve the quality of deliberative communities through effective participation and legitimacy of rules and standards, and consequently, the quality of political/societal systems or regimes.[22] Therefore, protecting and securing this data for use that does not harm deliberative communication is one of the top priorities of the emerging cyber regime. Bearing in mind that the number of internet users in 2000 was around 360 million users and today is around 2.5 billion, the urgency for setting up common norms and standards for internet to be used both by private and public actors and sectors, is high. Froomkin and others have long argued that due to the fact that communication between these users has risen dramatically over the past decades, deliberation theories

[19] Human Development Reports, 'Chapter 2: New Dimension of Human Security', (1994), 24. http://hdr.undp.org/en/reports/global/hdr1994/chapters/ (Access December 2013).

[20] Thomaz Guedes da Costa, 'Political Security, an Uncertain Concept with Expanding Concerns'in Hans Günter Brauch (ed.) *Globalization and Environmental Challenges. Reconceptualizing Security in the 21st Century* (Berlin: Springer, 2008) p.562 http://link.springer.com/chapter/10.1007%2F978-3-540-75977-5_42# (Access December 2013)

[21] International Telecommunication Union. 'Definition of cybersecurity' http://www.itu.int/en/ITU-T/studygroups/com17/Pages/cybersecurity.aspx ; Also *vid*. Tim Maurer, *Cyber Norm Emergence at the United Nations – An Analysis of the UN's Activities Regarding Cyber-security?* (Massachusetts: Belfer Center for Science and International Affairs, Harvard Kennedy School, 2011), p.8. http://belfercenter.ksg.harvard.edu/files/maurer-cyber-norm-dp-2011-11-final.pdf (Access December 2013).

[22] Michael Froomkin 'Habermas@Discourse. Net: Toward a Critical Theory of Cyberspace' (2003) 116 *Harvard Law Review*, 749-873.

might apply to explain what may happen next. Namely, due to the fact that people communicate more for professional, business or private reasons through the internet, they also exchange more ideas and opinions and thus create common norms and standards according to which they decide or govern their local environment. Consequently, global norms become local and vice a versa. This is also true for human rights standards. More people than ever have a common understanding today of privacy or freedom of expression or access to information and therefore share the same ideas and principles about what to express and how to protect and secure their private data. For example, the common wish to express religious ideas or political opinions without harming or insulting others or being insulted in one's own religious belief is a more common understanding among internet users today, than it was thirty years ago.

Nevertheless, according to the Freedom in the Net Index issued in 2013, most countries in the world censor Internet Freedom, some more, some less. There are various ways to do so. Governmental agencies, internet police or hackers-for-hire, use different methods to disturb, filter or censor the exercise of freedom rights. The Index cites that at least in 29 out of 60 states, blocking and filtering of information and platforms in the internet is a common practice.[23] Although not all countries in the world are covered in this index, the main industrial ones are and this indicates how virulent censorship is. Cyberattacks on dissidents and human rights advocates, or paid pro-government bloggers, i.e. in China, Bahrain or in Russia are a daily annoyance.

But the self-censorship that internet users impose upon themselves everywhere in the world is probably the most serious threat to internet freedom. Massive surveillance and misuse of our data in the internet and the fear that some of our private communication is made public, leads to self-censorship among internet users around the world. Individuals start to no longer use social networks or search engines to express their ideas or to search for certain keywords that may trigger the attention of national security agencies. They censor themselves in the way that they adapt to restrictive rules. This adaptive self-imposed censorship is not to be put on the same level as the 'do no harm' rule. The latter is about respect for the other person. Self-censorship is the fear of uncontrolled repercussions after expressing a view or opinion or looking up a keyword in a search engine. In this case, the internet becomes a political and manipulative tool, due to the fact that it can technically provide data on people's ideas to national security agencies or technical companies.

[23] Sanja Kelly, Mai Truong, Madeline Earp, Laura Reed, Adrian Shahbaz and Ashley Greco-Stoner (eds), *Freedom on the Net 2013. A Global Assessment of Internet and Digital Media* (Freedom House, 2013) http://freedomhouse.org/sites/default/files/resources/FOTN%202013_Full%20Report_0.pdf (Access December 2013).

Apart from this, the most common way to censor internet users is blocking and taking down web sites under governmental surveillance or deleting critical websites and social networks. Sometimes, security agencies cause the slowing down of the speed of internet, so people cannot use it for quick messages or search, for example, for protests, meeting points for demonstrations, urgent actions etc.. Thus, the freedom rights are under massive pressure and constant surveillance.

The president of Germany, Joachim Gauck, raised his concerns about this development in the internet during his annual address to the nation in 2013. Here within, he highlighted, that ‘all forms of privacy which our forefathers once used to fight for against the state, and which in totalitarian regimes helped us to shield ourselves from being coerced are fading away. Rather than posing a threat, publicity now seems to offer the hope of appreciation and recognition. (…) Many do not realize, or simply do not want to know that they are complicit in the creation of the virtual twin to their real life self – their alter ego who reveals, or could reveal, both their strengths and weaknesses, who could disclose their failures or deficiencies, or who could even divulge sensitive information about illnesses. Who makes the individual more transparent, readily analyzed and easily manipulated by agencies, politics, commerce and the labor market’.[24]

One way to face these challenges and guarantee more protection in cyberspace is the multi-stake holder approach, favored by many non-state actors in particular. This approach is about groupings of civil society actors, representatives from the private sector, the public sector, the media and other stakeholders that come together for a common purpose, namely to regulate communication in cyberspace. Over the past years different stakeholders, actors and agencies, such as representatives of search engines, communication platforms or social networks, to name but a few: Google, Skype, Microsoft Bing, Facebook, Twitter, Yahoo, Linkedin, Sina Weibo, Renren, Yandex or Yamli, have grouped themselves in different fora and networks. Search engines and social networks, for example, all have in common that they can allocate and collect data from each internet user, store it and later sell it or provide it for external users, such as private companies or national security agencies. The multi-stakeholder approach includes these companies and private actors as well representatives of international organizations such as the UN or the EU and national governments. They come together through informal and formal fora and build partnerships for consultation. One of these global internet fora is the Internet Governance Forum (IGF) mandated by the UN and by World Summit on the

[24] Speech by Federal President Joachim Gauck to mark the Day of German Unity Stuttgart, 3 October 2013, 4. http://www.bundespraesident.de/SharedDocs/Downloads/DE/Reden/2013/10/131003-Tag-Deutsche-Einheit-englische-Uebersetzung.pdf?__blob=publicationFile (Access December 2013).

Information Society (WSIS) in 2005 and founded in 2006. It has over 170 representatives of UN member states which are all convening this forum for a multi-stakeholder policy dialogue.[25] During their annual meetings they attain to develop a shared understanding about the protection of data in cyberspace but they nevertheless play different roles and have different purposes and aims in these fora and networks. Governmental representatives can make decisions, implement and enforce them. Others, like the consultance from private companies and NGOs, can only serve as advisors and experts in these fora. Their partnerships are voluntary, with participation driven by the perceived benefits they may see emerging from the process. They are increasingly being used to challenge and lobby for change in policy processes. They have already played a role on previous governmental agreements to protect copyrights or other data in cyberspace, such as 'IP Protection Act' Preventing Real Online Threats to Economic Creativity and Theft of Intellectual Property Act (PIPA) in 2008, or when passing the 'Stop online privacy act' (SOPA) in 2011 as well as during the 2012 attempt to set up an inter-governmental 'Anti-Counterfeiting Trade Agreement' (ACTA) on a global level. Copyright is an exclusive right an it has the potential to restrict freedom of expression, i.e. scientific knowledge on medicine, technologies, art or literature, by others than the holder or author of the copyright.[26]

Most of these recent efforts to protect copyrights where not successful because it became evident that governments alone cannot solve the problem of data protection. They need to join the multi-stakeholder approach that includes actors from the non-formal and private sector such as technical corporations, search engines, internet users, civil organizations, and so on. Therefore in 2011, the Council of Europe in Strasbourg expressed its concerns when highlighting that any internet governance arrangements must ensure the protection of all fundamental rights and freedoms and affirm their universality, interdependence, and interrelations in accordance with international human rights law. They must also ensure full respect for democracy and the rule of law and should promote sustainable development.[27] Therefore, in recent international meetings, we find a mix of actors and stakeholders involved in international, regional or national, for example IGOs, states, CSOs, technical actors that represent providers, communication services or search engines such as Microsoft, Apple, Google, Firefox, Yahoo, Xando, Weibo, Skype, Clouds, Dropbox etc. or other private business actors such as online business and companies, start-ups, different App provides, Amazon, DHL, or network

[25] Internet Governance Forum, http://www.intgovforum.org/ (Access December 2013).

[26] Ellen M. Wesselingh, The magic show of balancing the enforcement of copyright and freedom of expression, Proceedings of the International Conference on ICT Law 2013, unpublished article, 15 August 2013.

[27] Council of Europe, 'Declaration by the Committee of Ministers on Internet governance principles', 21 September 2011. Also *vid.* Wolfang Kleinwächter (ed.), *Human Rights and Internet Governance*, (Berlin: Internet and Society Co:llaboratory e.V, 2012), 7. http://dl.collaboratory.de/mind/mind_04berlin.pdf (Access December 2013).

actors like Mxit, Wretch, Facebook, Nexopia, Google+, Badoo, XING, Hi5, Orkut, Renren, Linkedin, Skype and so on. The list could be continued. Implicitly, the internet user is involved in all these categories and can have multiple functions, for example, when being a user of Renren, a customer of DHL, and working for IBM. Therefore her or his data can be collected by multiple technical providers, engines or companies during every phase of one's own life.

In the context of cybersecurity, internet control is an array of measures that lead to technical blocking (IP and URL blocking); removing search results; the take-down by regulators often according to national law, for example, in 2011 in Egypt during the revolts and in 2009 in Iran during student protests; or through self-censorship based on fear and threats of legal actions, group pressure, or intimidation by governments.[28] Self-censorship is one of the most restrictive measures as mentioned earlier. It means that people start censoring their own internet usage in order to abide by norms and thus restrict their own freedom rights. One example of a regional inter-governmental regime that aims to restrict more freedom rights in the internet is the Shanghai Cooperation Organization (SCO). The member states of SCO coordinate policies and protective integration against democracy, regime change and human rights in cyberspace.[29] Consequently, the trust and confidence in state authorities of internet users living and working in these countries is most likely to decrease. Trust and personal engagement through data protection, for example, when asking: 'Is my data safe? Do I understand what is happening with it?' is crucial. Global cyberspace norms will more likely be adhered to by all internet-users if they have been part of designing them and agreeing upon them. This will enhance the legitimacy and authority of institutions, organizations, companies, agencies and practices in cyberspace.[30] Frequent and widespread national data surveillance programs instead jeopardize civic trust and confidence in the internet. They are conducted by national security agencies, secret services or private companies. Governments and national authorities using national intelligence or spyware viruses, or private corporations using business intelligence, can modify cookies on private computers to deduct data for their own purposes. Every internet users leaves long data trails through social networks, i.e. on Skype and Facebook, after online shopping, when using governmental information services, or

[28] OpenNet Initiative. https://opennet.net/ (Access December 2013).

[29] Shanghai Cooperation Organization. http://www.sectsco.org/EN123 (Access December 2013). Members and observers: China, Kyrgystan, Kazachstan, Russia, India, Iran, Mongolia, Afghanistan, Prakistan, Belarus, Turkey, Uzbekistan, Sri Lanka and Tajikistan.

[30] William E. Hornsby, Jr, 'The Ethical Boundaries of Selling Legal Services In Cyberspace'(1996) *National Law Journal* http://www.kuesterlaw.com/netethics/abawill.htm (Access December 2013); Also *vid*. Joe Peppard and Anna Rylander, 'Products and service in Cyberspace'(2005) 25 *International Journal of Information Management*, 335-345. https://dspace.lib.cranfield.ac.uk/bitstream/1826/2687/1/Products%20and%20Services%20in%20cyberspace%20-%202005.pdf (Access December 2013).

while sending SMS and other private messages through Email. We leave data trails when applying for new IDs online, using credit cards and so on. The amount of data is massive, hardly anyone has an oversight over it and therefore the abuse and misuse of these data is so alarming. We are no longer the owner of our own private data, and that is what leads to misconducts in cyberspace. It is massively used and processed by other stakeholders, both private and public ones.[31] No single government has control over all this data, not even the most democratic societies, and this is why this data-trail also poses a threat to democracy and good governance. The fact that we cannot be assured protection leads to mistrust in companies or national authorities and thus decreases legitimacy of governments and other authorities.

Security issues are often connected to warfare and also cyberwarfare. This is a term that expresses the combination of technical warfare instruments in cyberspace. The term had already curbed in 1993.[32] This type of cyberwarfare involves the actions by a state, i.e. national military or international organizations (i.e. NATO[33]) to attack another nation's computers or information networks through, for example, computer viruses.[34] In response to the dramatic rise of expenditures for cyberwarfare and cybercontrol by all countries around the world, the UN Security Council Working Group Report 2013 urges all UN member states to make careful risk assessment in cyberspace, i.e. control and vigilante cyberattacks through hackers. These attacks can dramatically affect national infrastructure and destroy a whole country, for example, through ICT-enabled industrial control systems of nuclear power plants. Furthermore, if governments and other actors were to invest more in confidence-building measures in the cyber domain, i.e. transparency, participation, consultation with ASEAN, AU, Arab League, OSCE, the NATO or the EU, in adopting cybersecurity policies, that would help to regain trust of internet-users. Otherwise, so the concern, cybersurveillance becomes a

[31] Forrest Hare, 'Borders in Cyberspace: Can Sovereignty'Adapt to the Challenges of Cyber Security?'in Christian Czosseck, Kenneth Geers (ed.) *The Virtual Battlefield: Perspectives on Cyber Warfare (2009) Cryptology and Information Security Series Vol.3* Amsterdam: IOS Press.
http://www.ccdcoe.org/publications/virtualbattlefield/06_HARE_Borders%20in%20Cyberspace.pdf (Access December 2013).
Electronic Frontier Foundation: https://www.eff.org/deeplinks/2013/06/internet-and-surveillance-UN-makes-the-connection (Access December 2013).

[32] John Arquilla and David Ronfeldt, 'Cyberwar is Coming!' (1993) 12 *Comparative Strategy,* 141-165

[33] NATO Cooperative Cyber Defense Center of Excellence, Tallin, Estonia. https://www.ccdcoe.org/ (Access December 2013). Also *vid.* Katharina Ziolkowski (ed.) *Peacetime Regime for State Activities in Cyberspace* (to be published in the end of 2013).

[34] Tim Maurer, *Cyber Norm Emergence at the United Nations – An Analysis of the UN's Activities Regarding Cyber-security* (Massachusetts: Belfer Center for Science and International Affairs Harvard Kennedy School, 2011), 15.
http://belfercenter.ksg.harvard.edu/files/maurer-cyber-norm-dp-2011-11-final.pdf

dangerous weapon against citizens, companies, and countries without control.[35] In this context it is national security agencies or the military which harms and violates human rights in cyberspace. For example, after 9/11 anti-terror internet surveillance measures in Europe, the USA, China, Russia, Saudi Arabia, Kenya and way over 100 countries worldwide have increased dramatically. In India after the 2008 terror attack in Mumbai, the government passed the Information Technology Rules in 2011 which states that 'anyone who finds certain web content objectionable now has the right to have that site shut down.'[36]

In a 'real war' either the Head of State or the Defense Minister of a nation would publically declare action or explain further steps. In this wrongly labeled cyber war there is no Defense Ministry visible so far. In Germany it has been the Minister for Internal Affairs' duty to respond, in the UK the Security Service, in the US the White House, and so on to express their concerns about cybersecurity.[37] This means that governments reassume sovereignty and control over whistleblowers and leaks and others. Yet, the fact that NATO has put the issue of cyber war on the agenda and is one of the main promoters of this notion of cyberwarfare shows that the debate has reached all levels of international and national affairs. Military and national security expenditure have dramatically risen over the past years, so in Saudi Arabia and the US under the label to fight cyber-crime through cyberwarfare.

Cyberespionage is often mentioned in the context of cybersecurity and cyberwarfare. It describes the stealing of national intelligences or industrial data stored in digital formats on computers and IT networks. This affects all industrial and public sectors, for example scientific results or intellectual property through computer viruses. Different from these 'internet spies' are the cases of whistleblowers to be seen. Whistleblowers are private persons or agencies which expose misconduct in an organization such as a governmental agency (e.g. NSA) or private company, for example Apple or Google or other power grids. They argue that these misconducts, i.e. collecting private data of citizen's and presidents of other countries, violate general and common rules, such as human rights norms and standards, such as the  chief engineer of the Water Resource Department in a state in India, Vijay

[35] Detlev Wolter, 'The UN takes a big step forward on Cybersecurity', September 2013. http://www.armscontrol.org/act/2013_09/The-UN-Takes-a-Big-Step-Forward-on-Cybersecurity

[36] Radio Netherlands Worldwide. Declarations of Gerard Oonk, director of  the Dutch NGO The India Committee of the Netherlands, 5 May 2011.  http://www.rnw.nl/english/article/stricter-indian-internet-laws-threaten-human-rights (Access December 2013).

[37] Catherine Lotrionte (2012) State Sovereignty and Self-Defense in Cyberspace: A Normative Framework for Balancing Legal Rights, *Emroy International Law Review*, Vol. 26, Issue 1, 825-919. http://www.law.emory.edu/fileadmin/journals/eilr/26/26.2/Lotrionte.pdf (Access December 2013).

Pandhare, in 2012[38]; or the scandal around the US-NSA subcontractor Edward Snowden in 2013. They both claimed to have made public the misconduct of citizens' data for private national security reasons that were not justified or legitimized under the law – let alone international human rights law. Recommendation to improve security in cyberspace thus goes so far as to increase the access to information and transparency and confidence building, improve and spread internet and cyberspace literacy of citizens and to encourage for more participation through CSOs and multi-stakeholder approach.[39]

## E-GOVERNANCE, E-GOVERNMENT AND E-DEMOCRACY

E-Governance is citizen and user driven and applies to private companies, governments, social networks or NGOs, that is to say, any organization, institution or company. It aims to reach the beneficiary, i.e. the internet user, and ensure that the services intended, i.e. through search engines, governments etc., reach the desire of the individual. There is an auto-response system to support the essence of E-Governance, whereby national authorities ought to guarantee the efficacy of E-Governance by setting the legal and political frameworks. E-Governance is by the governed, for the governed and of the governed based on good governance principles. Recent statistics have shown that countries with high levels of social capital and technical infrastructures use E-Governance more than countries with less infrastructures.[40] Consequently, E-Democracy is using information and communications technology (ICT) to promote democratic behavior and actions. It allows internet users to use ICT to participate equally in the proposal and the larger decision making process on the local, national or international level. This participation via internet can result in common agreements, norms, rules and laws to govern communities. Tools for E-Democracy ought to be free, easily accessible, and allow for equal practice of political self-determination. Therefore it is shown that countries who score

[38] Susan Landau, 'Making sense from Snowden: What's Significant in the NSA Surveillance Revelations'(2013) 11 *IEEE Security & Privacy* 66-75. Also *vid.* Down to Earth, 'Reservoir of Corruption' 31 October 2012, http://www.downtoearth.org.in/content/reservoir-corruption (Access December 2013).

[39] Ronald J. Deibert and Masashi Crete-Nishihata, 'Global Governance and the Spread of Cyberspace Controls' (2012) 18 Global Governance 339-361. http://citizenlab.org/cybernorms2012/governance.pdf (Access December 2013). International Telecommunication Union. World Map: http://www.itu.int/en/ITU-D/Statistics/Documents/facts/ICTFactsFigures2013.pdf (Access December 2013).

[40] United Nations, *E-Government Survey 2012. E-Government for the people* (New York: 2012), 9ff. http://unpan1.un.org/intradoc/groups/public/documents/un/unpan048065.pdf (Access December 2013).

high on E-Democracy also score high on democracy in general.[41] Thus, there is a correlation between technical infrastructure that allows for a majority of citizen to use the internet as one tool, among others, to participate in the public decision making process. That is what democracy is in a nutshell. Yet, there is no evidence and no causality that E-Democracy leverages democratic behavior per se in countries that score generally low in democracy or are governed in an autocratic manner. Because E-Democracy is only another way in which to build upon already existing good governance principles such as accountability/ responsiveness, transparency and internet citizen participation, here is no automatism or automatic causality between internet access and democracy. But the access to internet, which provides access to information and participation can be a tool or catalyst to trigger changes in society that eventually lead to more democratic ways to govern a society. Modernization theorists would argue that due to the fact that internet access needs a good technical infrastructure, the likeliness for also democratic development is higher in countries where people have access to cyberspace than in countries where this access is limited.[42]

The core question remains, whether or not people can develop trust and confidence in these internet “tools” that can leverage democracy. In order to draw a correlation we can take a look at the general definition of democracy. Now it becomes evident that cyberspace and E-Democracy technology, search engines, network providers etc., can be used as tools or catalysts but they do not automatically build up a democratic culture or country; because democracy is one form of governance in which all citizens participate equally and freely to agree on common norms and standards, either directly or through representation, which lead to the creation of rules and laws under which they wish to be governed. It is the “rule of the people” for the people (Greek: *demokratia*), which today also results in the concept of “rule of law” as the basis for any democratic regime. Therefore, it depends how all people in society use these tools or have access to them. Therefore, E-Governance and E-Government are some of the tools that are expected to reach a higher acceptance in the years to come and that can – but do not automatically – lead to more democracy and greater adherence to the Rule of Law, and consequently human rights.

During the debates about the Post 15+ UN Sustainable Development Goals (SDGs) the idea of increasing E-Governance around the world, in order reach socio-economic development and human rights, played a fundamental role. The UNDP seeks it as a major tool in achieving the SDGs, because

[41] Irina Netchaeva ‘E-Government and E-Democracy. A Comparison of Opportunities in the North and South’(2002) 64 *The International Journal for Communications Studies* 467-477.

[42] Sheri Berman, ‘What to Read on Modernization Theory’, *Foreign Affairs* (2009) http://www.foreignaffairs.com/features/readinglists/what-to-read-on-modernization-theory (Access December 2013)

E-Governance can support the implementation process of human rights in all aspects of life: health, governance, environment, cyberspace and so on. This new framework is member state-led with participation from external stakeholders such as civil society organizations, the private sector and businesses, as well as academia and scientists. It can ensure that public institutions are effective, responsive, accountable and representative through E-Government and other E-Governance means. This includes fostering public sector capacities and public-private partnerships at national and subnational levels; strengthening regulatory framework for businesses; preventing corruption; and promoting the transparent and sustainable management of public goods and financial and natural resources.[43]

International Relations and Regime Theories, as led by constructivist and globalization theorists, have long highlighted the fact that norms impact state and non-state actors' behavior also in cyberspace. They argue that international norms can shape, and at the same time constrain, access to information and communication in business, politics, family or other private matters. They include an array of technologies, regulatory measures, laws, policies and tactics for commercial, political or private reasons beyond border control but based on norm diffusion.[44] The UN as well as the EU and other inter-governmental organizations such as the SCO, have therefore launched a number of declarations or binding agreements on how to use or combat misuse of data in cyberspace and yet allow citizens free and open access to information, which is among their basic human rights. Some of these agreements resulted in the protection, and others in the violation, of human rights. Recently, there have been some UN Resolutions on 'cyber security' that are worth taking a closer look at later. Although major players in this arena such as Russia and China do not want legally binding treaties, they also support these developments. Instead, social networks play an interesting role in this arena. Some call them the new social movements beyond legislations, because their 'members' and stakeholders (the internet users) are visible and thus dare to show and express their claims and desires to freely communicate in a transparent way. Therefore these networks and movements cannot be declared anti-democratic just because they act beyond state borders or statehood. Instead they share global values, among which the human rights values and norms are the most common ones. The fact that many monitoring institutions set agendas, such as the Freedom house index on the "Freedom of Net" to assess whether a society enjoys freedom to information, association or privacy, is not surprising. The

[43] Human Rights Office of the High Commissioner, 'Global Consultation on Governance and the Post-2015 framework' 7 October 2012, http://www.worldwewant2015.org/node/277876 (Access December 2013).

[44] Ronald J. Deibert and Masashi Crete-Nishihata, 'Global Governance and the Spread of Cyberspace Controls'p.349.

LSE media platform established in 2011 deals with these issues, aiming to assess the relationship between media communication, networks, and individual stakeholders, and how they solve and govern challenges and problems.[45]

These initiatives also indicate that social networks are horizontal in structure, as opposed to governmental and sovereign states, which act entirely vertical and hierarchal. In any cyber-war scenario there will be no end, because weappons (cybervirsuses) are endless and repetitive, no peace contract because there are no real opponents who could contract and thus, it has to be dealt with differently, and we do not yet know how. Nevertheless, there is a creation of a global virtual enemies in persons such as the WikiLeaks founder, Assange, or the whistleblower, Snowden, and others which usually have a face and a name that become a symbol or target for the debate on cybersecurity. Governments often label these individuals as security threats. They are proxies that resemble that governments fear to lose control over cyberspace – which they probably never controlled in the first place. At the end the cybersecurity, surveillance, or war is about whether human freedom succeeds over statehood.

## HUMAN RIGHTS COMPLIANCE

To safeguard human rights in cyberspace it takes various actors and agencies, and yet, governmental authorities and democratic institutions are fundamental to do so. National and international courts can play a crucial role and are part of this cyberregime to protect human rights. For example in 2010, the Supreme Court of Costa Rica ruled in one case that access to ICT becomes a basic tool to facilitate the exercise of fundamental rights and democratic participation (E-Democracy) and citizen control, education, freedom of thought and expression, access to information and public services online, the right to communicate with government electronically and administrative transparency, among others. This includes the fundamental right of access to these technologies, in particular, the right of access to the Internet or World Wide Web.[46] Judges did not need to create new cyber law to protect human rights, they applied common norms and international human rights law to cases concerning cyberspace and therefore guaranteed access to information and communication as a basic human right. Similarly,

[45] London School of Economics Media Policy Project http://blogs.lse.ac.uk/mediapolicyproject/programme/ (Access December 2013).

[46] Supreme Court of Costa Rica, Res. Nº 2010012790, 30 July 2010, Considerando V.

in a case concerning Turkey in 2012, the European Court of Human Rights (ECtHR) has reinforced the right of individuals to access the internet through a ruling against wholesale blocking of online content, asserting that the internet has now become one of the principal means of exercising the right to freedom of expression and information.[47] The judges in Strasbourg ruled on a benchmark case, which established relevance for the arguments against such human rights violations. And in 2013 the same court set yet other groundbreaking standards for the internet. In October 2013 the European Court of Human Rights ruled that an Estonian news portal, Delfi, was responsible for offensive anonymous posts after it had reported about a ferry company. In 2010 the Estonia's Supreme Court ruled that the website was responsible for the comments, not the people who made them and the judges in Strasbourg backed that stance in 2013.[48] In consequence that means, that service providers, website owners and others will be held accountable of what 'their users' or visitors post inadequate language on their websites that violates the dignity, privacy of others or statement that are simple false or impede the progress or development of third parties – as was the case in Estonia. If false allegations or harmful expressions against others appear on the internet, the owner or provider of the website can be held responsible for it.

Similar to the  concept of corporate social responsibility -in which private companies have to ensure that human rights are guaranteed and standards upheld among their employees, in their products, in their marketing concepts and for their customers – the concept of human rights in cyber space works. Everyone who uses internet and makes use of cyberspace has the responsibility to protect and respect private data and freedom of information. The internet users, providers, companies or governments alike can be made responsible for violating rights and also for protecting them.  That is to say, individuals, companies or governmental authorities who violate one's privacy can be held accountable through institutions, such as authorities and courts in the countries or unions (AU, EU, OAS, etc.) they are resident of. Any international or global agreement that manifests human rights in cyberspace ought to be co-signed by all stakeholders such as social networks and governments alike, further encouraging their compliance to it. Such an agreement only makes sense if every country becomes party to. So far, governments and national institutions are still the strongest enforcement mechanisms to guarantee the rights of their citizens and enforce them if needed.

The major challenge for human rights compliance in cyberspace is the question of state sovereignty and legitimacy. The issue of legitimacy is so far primarily seen in the context of physical

[47] ECtHR, *Case Yildirim v.Turkey,* 18 December 2012, para.54.
[48] ECtHR, *Case Delfi As v. Estonia,*  10 October 2013.

and territorial based state institutions, organizations or other legal entities. It has not been widely debated among internet users on the global level.  But one can argue, that by making use of services in the internet (governmental or private ones) they grant legitimacy to them. If they abstain from making use of them, they delegitimize them. Sovereignty is state-based and connected to jurisdiction over a specific territory, i.e. when exercising international human rights law. And legitimacy of any institution, company or organization is achieved through the level of civic engagement or interaction in setting up, adhering to or accepting common rules and standards. It increases or decreases by the level of internet users' trust in or engagement with these entities. The more these entities comply with its commands and human rights, the higher their legitimacy will be. Therefore, these entities enjoy high legitimacy when applying good governance principles in any business or technical companies, governments or CSO, online as well as offline.[49]

Globalization and constructivist approaches help us to understand why some argue that norm and human rights diffusion impacts the way national jurisdiction (also in the case of cybercrimes) applies and changes the way we think about state borders and nation state as such. Global cyber governance regime is legitimate and sovereign if we interact on different levels.[50] One element of this regime is that  this national jurisdiction can serve as a lawful power to make enforce rules. It implies that everyone has the duty to protect human rights in cyberspace as derived from the principle of territorial sovereignty. The International Court of Justice (ICJ) has, for example, argued that territorial sovereignty also implies obligations to protect human rights in cyberspace, i.e. if they get violated by technical companies or servers that are based within one's own territory, because even cyberspace requires the existence of some physical architectures, somewhere.[51] In response to this debate whether internet can weaken or strengthen sovereignty and legitimacy of state institutions, the UN Special Rapporteur de la Rule recommended states to review national laws regulating surveillance and update

[49] Jonathan Weinberg, 'Non-State Actors and Global Informal Governance — The Case of ICANN', in Thomas Christiansen and Christine Neuhold (eds.) *International Handbook on Informal Governance* (Massachusetts: Edward Elgar Publishing, 2012)
http://jotwell.com/exploring-legitimacy-in-internet-institutions/ (Access December 2013).

[50] Wolff Heintschel von Heinegg, 'Legal Implications of Territorial Sovereignty in Cyberspace' (2012) 4 *International Conference on Cyber Conflict*, 7-19
http://www.ccdcoe.org/publications/2012proceedings/1_1_von_Heinegg_LegalImplicationsOfTerritorialSovereigntyInCyberspace.pdf (Access December 2013).

[51]  Wolff Heintschel von Heinegg,  'Territorial Sovereignty and Neutrality in Cyberspace' (2013) 89 *International Law Studies*, 123-156 http://www.usnwc.edu/getattachment/ff9537ce-94d6-49a8-a9ef-51e335126c1e/von-Heinegg.aspx (Access December 2013);
Wolff Heintschel von Heinegg, 'Legal Implications of Territorial Sovereignty in Cyberspace' p.15-17.
http://www.ccdcoe.org/publications/2012proceedings/1_1_von_Heinegg_LegalImplicationsOfTerritorialSovereigntyInCyberspace.pdf (Access December 2013).

and strengthen laws and legal standards. Communications surveillance should be regarded as a highly intrusive act that potentially interferes with the rights to freedom of expression and privacy and threatens the foundations of a democratic society. Legislation must stipulate that state surveillance of communications must only occur under the most exceptional circumstances and exclusively under the supervision of an independent judicial authority.[52]

**SUMMARY: RULE OF LAW IN CYPERSPACE?**

Ultimately, Public Privacy is a new trend in which a global public of internet users aims to uphold their basic human rights through good governance principles in cyber space. International jurisdiction, customary and international human rights law, and the shifting role of duty-bearer and right-holders towards more individual responsibility are all part of the recent development towards an open and fair cyber-governance regime. Furthermore, it is about combating injustice, abuse and misuse of data in cyberspace. The concept of Public Privacy encompasses various human rights norms and standards. Governments or governmental authorities and national legislation in adherence to international human rights law have, so far, the primary responsibility to protect human rights and thus privacy rights in cyberspace. Due to their national and international jurisdiction, i.e. through independent courts, they also have adequate enforcement mechanism in place. Others such as technical companies, CSOs and search engines like Google, Microsoft or Digital Rights Watch are claimed to be co-responsible for the way personal and business data is processed, made public, protected or otherwise dealt with. Yet, parallel to the multi-stakeholder approach the claims for multiple or shared responsibilities emerge. Legal and political research on how shared responsibilities among the different stakeholders to be held accountable for human rights compliance and other norm compliance in a borderless world are currently under way.[53]

While there is no lack of human rights standards or law, the deficits lay in the measures and mechanisms that allow us to comply and adhere to these standards. They are national not global, let alone cyber. Therefore the global cyberregime has to develop innovative ways and mechanisms to

[52] UN Doc. A/HRC/23/40. Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue, 17 April 2013, para.81 http://www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session23/A.HRC.23.40_EN.pdf (Access December 2013).

[53] SHARES, The Research Project on Shared Responsibilities in International Law http://www.sharesproject.nl/ (Access December 2013).

monitor and enforce global human rights standards that go beyond existing national measures. There might be different ways to do so without excluding existing legal or political mechanisms.

One suggestion which has been proposed in this paper is the multi-stakeholder approach. The existing common global guidelines and laws ought to be framed for the needs and purpose of internet users by a multi-stakeholder community, regional organizations and internet users. This might more likely guarantee the inclusion of the 'public' (the internet users) and the protection of our privacy, namely our civic and social human rights  in the context of health, family, work, information, communication, etc.. The question of cyberjustice, for example, is adding to this debate. It seems ICT is a key component of good governance and democracy, but to administrate it is difficult. To transfer, for example, trials to the internet can speed and strengthen up justice processes and procedures but therefore data has to be safe and secure, for example, for testimonials in front of the court through the internet or mobile phones, for example.[54] Nevertheless, if it is technical possible, it might be one innovative way to attain justice and protection of human rights in cyberspace. If the stakeholders who work on more cybersecurity succeed in finding ways and tools to secure data and freedom, they will implicitly create a rule of law by internet users for internet users.

A non-legally binding UN Resolution from November 2013[55] indicates exactly the above mentioned developments and efforts - namely that member states emphasize that illegal surveillance of communications, their interception and the illegal collection of personal data constitute a highly intrusive act that can violate the right to privacy and freedom of expression and may threaten the foundations of a democratic society.  With this resolution, UN member states recall their own obligation to ensure that measures taken to counter terrorism or other security threats comply with international human rights law. Therefore, the 2013 UN resolution calls upon states to take measures to put an end to violations of those rights and specifically to establish independent oversight mechanisms capable of ensuring transparency and accountability of state surveillance of communications, their interception and collection of personal data. It is the urge for a new rule of law in cyberspace. That is to

[54] University of Montreal 'World Bank draws on expertise of Université de Montréal's Cyberjustice Laboratory' 11 February 2013. http://www.nouvelles.umontreal.ca/udem-news/news/20130211-world-bank-draws-on-expertise-of-universite-de-montreals-cyberjustice-laboratory.html (Access December 2013).
Philip Kastner 'Cyberjustice in the Context of Transitional Justice'(2013) 9 *Cyberjustice Laboratory Working Papers* http://www.laboratoiredecyberjustice.org/Content/documents/WP009_TransitionnalJusticeAndCyberjustice_en.pdf (Access December 2013).
Action Committee on Access to Justice in Civil and Family Matters, *A Roadmap for Change* (Ottawa, 2013) http://www.laboratoiredecyberjustice.org/Content/documents/ac_report_-_english_october_8_2013.pdf (Access December 2013).

[55] UN Doc. A/C.3/68/L.45. General Assembly, 'The right to privacy in the digital age', 1 November 2013.

say within the borderless, but yet largest ‘cybercountry’ of 2.5 billion inhabitants (and very rapid population growth) on this planet, the need for new institutional set ups that govern, regulate and manage this space is enormous.

## BIBLIOGRAPHY

### Books

- Guedes da Costa, Thomaz, ‘Political Security, an Uncertain Concept with Expanding Concerns’in Hans Günter Brauch (ed.) *Globalization and Environmental Challenges. Reconceptualizing Security in the 21st Century* (Berlin: Springer, 2008) p.562 http://link.springer.com/chapter/10.1007%2F978-3-540-75977-5_42#
- Hare, Forrest, ‘Borders in Cyberspace: Can Sovereignty’Adapt to the Challenges of Cyber Security?’in Christian Czosseck, Kenneth Geers (ed.) *The Virtual Battlefield: Perspectives on Cyber Warfare - Cryptology and Information Security Series Vol.3* (Amsterdam: IOS Press, 2009) http://www.ccdcoe.org/publications/virtualbattlefield/06_HARE_Borders%20in%20Cyberspace.pdf
- Kelly, Sanja, Truong, Mai, Earp, Madeline, Reed, Laura, Shahbaz, Adrian, Greco-Stoner, Ashley (eds), *Freedom on the Net 2013. A Global Assessment of Internet and Digital Media* (Freedom House, 2013) http://freedomhouse.org/sites/default/files/resources/FOTN%202013_Full%20Report_0.pdf
- Kleinwächter, Wolfang (ed.), *Human Rights and Internet Governance*, (Berlin: Internet and Society Co:llaboratory e.V, 2012) .http://dl.collaboratory.de/mind/mind_04berlin.pdf
- Maurer, Tim, *Cyber Norm Emergence at the United Nations – An Analysis of the UN‘s Activities Regarding Cyber-security* (Massachusetts: Belfer Center for Science and International Affairs Harvard Kennedy School, 2011), http://belfercenter.ksg.harvard.edu/files/maurer-cyber-norm-dp-2011-11-final.pdf
- Office of the High Commissioner for Human Rights, *Human Rights Indicators: A Guide to Measurement and Implementation* (Geneva: 2013) https://unp.un.org/Details.aspx?pid=23745

- Weinberg, Jonathan, 'Non-State Actors and Global Informal Governance — The Case of ICANN', in Thomas Christiansen and Christine Neuhold (eds.) *International Handbook on Informal Governance* (Massachusetts: Edward Elgar Publishing, 2012) http://jotwell.com/exploring-legitimacy-in-internet-institutions/
- Ziolkowski, Katharina (ed.) *Peacetime Regime for State Activities in Cyberspace* (to be published in the end of 2013).

**Journal Articles**

- Arquilla , John, Ronfeldt, David 'Cyberwar is Coming!' (1993) 12 *Comparative Strategy,*
- Berman, Sheri, 'What to Read on Modernization Theory', *Foreign Affairs* (2009) http://www.foreignaffairs.com/features/readinglists/what-to-read-on-modernization-theory
- Deibert, Ronald J., Crete-Nishihata, Masashi, 'Global Governance and the Spread of Cyberspace Controls' (2012) 18 *Global Governance.* http://citizenlab.org/cybernorms2012/governance.pdf
- Froomkin, Michael, 'Habermas@Discourse. Net: Toward a Critical Theory of Cyberspace' (2003) 116 *Harvard Law Review*.
- Heintschel von Heinegg, Wolff, 'Legal Implications of Territorial Sovereignty in Cyberspace' (2012) 4 *International Conference on Cyber Conflict,*
- Hornsby, Jr, William E., ' The Ethical Boundaries of Selling Legal Services In Cyberspace'(1996) *National Law Journal* http://www.kuesterlaw.com/netethics/abawill.htm
- Kastner, Philip, 'Cyberjustice in the Context of Transitional Justice'(2013) 9 *Cyberjustice Laboratory Working Papers* http://www.laboratoiredecyberjustice.org/Content/documents/WP009_TransitionnalJusticeAndCyberjustice_en.pdf
- Kiskis, Mindaugas, (2011) 'Entrepreneurship in Cyberspace: What do we know? (2011), *Social Technologies*, Mykolas Romeris University, 1 (1), 37-48.
- Lotrionte, Catherine, 'State Sovereignty and Self-Defense in Cyberspace: A Normative Framework for Balancing Legal Rights' (2012) *Emroy International Law Review*, Vol. 26, Issue 1, 825-919. http://www.law.emory.edu/fileadmin/journals/eilr/26/26.2/Lotrionte.pdf
- Netchaeva, Irina 'E-Government and E-Democracy. A Comparison of Opportunities in the North and South'(2002) 64 *The International Journal for Communications Studies* 467-477.

- Nissenbaum, Helen, 'Toward an Approach to Privacy in Public: Challenges of Information Technology (1997) 7 (3), *Ethics & Behavior*, 207-219. http://www.nyu.edu/projects/nissenbaum/papers/toward_an_approach.pdf
- Landau, Susan, 'Making sense from Snowden: What's Significant in the NSA Surveillance Revelations'(2013) 11 *IEEE Security & Privacy*.
- Peppard, Joe, Rylander, Anna, 'Products and service in Cyberspace'(2005) 25 *International Journal of Information Management*, 335-345. https://dspace.lib.cranfield.ac.uk/bitstream/1826/2687/1/Products%20and%20Services%20in%20cyberspace%20-%202005.pdf
- Wesselingh, Ellen M. The magic show of balancing the enforcement of copyright and freedom of expression, Proceedings of the International Conference on ICT Law 2013, unpublished article (15 August 2013).

**International Organization's Documents**

- Council of Europe, 'Declaration by the Committee of Ministers on Internet governance principles', 21 September 2011.
- Human Development Reports, 'Chapter 2: New Dimension of Human Security', (1994) http://hdr.undp.org/en/reports/global/hdr1994/chapters/
- UN Doc. A/HRC/20/L.13. Human Rights Council, "The promotion, protection and enjoyment of human rights on the Internet", 29 June 2012.
- UN Doc, GA A/CONF.157/24 (Part I), Report of the World Conference on Human Rights by the UN Secretary-General, October 1993 http://www.unhchr.ch/Huridocda/Huridoca.nsf/(Symbol)/A.CONF.157.24+(Part+I).En
- Human Rights Office of the High Commissioner, 'Global Consultation on Governance and the Post-2015 framework' 7 October 2012, http://www.worldwewant2015.org/node/277876
- Office of the High Commissioner for Human Rights, 'Human Rights Indicators: A Guide to Measurement and Implementation' (Geneva, 2013)
- UN Doc. A/C.3/68/L.45 General Assembly, 'The right to privacy in the digital age', 1 November 2013.
- UN Doc. A/HRC/23/40, Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue, 17 April 2013

- UN Doc. A/HRC/17/27. Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue, 16 May 2011.
- UN Doc. General Assembly Resolution 217 A (III). Preamble of the Universal Declaration of Human Rights. December 1948.
- United Nations, *E-Government Survey 2012. E-Government for the people* (New York: 2012), http://unpan1.un.org/intradoc/groups/public/documents/un/unpan048065.pdf

**Internet Sources**

- Action Committee on Access to Justice in Civil and Family Matters, 'A Roadmap for Change' (Ottawa, 2013) http://www.laboratoiredecyberjustice.org/Content/documents/ac_report_-_english_october_8_2013.pdf
- Business and Human Rights Resource Center, 'Ranking Digital Rights project': http://www.business-humanrights.org/Documents/Ranking_Digital_Rights
- Detlev Wolter, 'The UN takes a big step forward on Cybersecurity', (2013). http://www.armscontrol.org/act/2013_09/The-UN-Takes-a-Big-Step-Forward-on-Cybersecurity
- Down to Earth, 'Reservoir of Corruption' 31 October 2012. http://www.downtoearth.org.in/content/reservoir-corruption
- Electronic Frontier Foundation, 'Internet Surveillance and Free Speech: the United Nations Makes the Connection' (2013). https://www.eff.org/deeplinks/2013/06/internet-and-surveillance-UN-makes-the-connection
- Council of Europe, ECtHR, Research Division (2011) 'Internet: Case-law of the European Court of Human Rights, Strasbourg, June 2011 www.echr.coe.int
- Jacob Appelbaum, 'Elevate Open Everything' in *Elevate Festival Opening Speech*, (2013). http://2013.elevate.at/festival/ueber-das-festival/newsmagazin/detail/news/jacob-appelbaum-elevate-open-everything/
- Jeff Jarvis 'A Bill of Rights in Cyberspace', 27 March 2010. http://buzzmachine.com/2010/03/27/a-bill-of-rights-in-cyberspace/ (Access December 2013)
- John Perry Barlow, 'A Declaration of the Independence of Cyberspace', (1996). https://projects.eff.org/~barlow/Declaration-Final.html
- International Telecommunication Union. 'Definition of cybersecurity', http://www.itu.int/en/ITU-T/studygroups/com17/Pages/cybersecurity.aspx

- International Telecommunication Union. World Map: http://www.itu.int/en/ITU-D/Statistics/Documents/facts/ICTFactsFigures2013.pdf
- Internet Governance Forum, http://www.intgovforum.org/
- NATO Cooperative Cyber Defense Center of Excellence, Tallin, Estonia. https://www.ccdcoe.org/
- London School of Economics Media Policy Project. http://blogs.lse.ac.uk/mediapolicyproject/programme/
- OpenNet Initiative. https://opennet.net/
- Radio Netherlands Worldwide. Declarations of Gerard Oonk, director of the Dutch NGO, The India Committee of the Netherlands, 5 May 2011. http://www.rnw.nl/english/article/stricter-indian-internet-laws-threaten-human-rights
- Shanghai Cooperation Organization. http://www.sectsco.org/EN123
- Speech by Federal President Joachim Gauck to mark the Day of German Unity Stuttgart, (2013), http://www.bundespraesident.de/SharedDocs/Downloads/DE/Reden/2013/10/131003-Tag-Deutsche-Einheit-englische-Uebersetzung.pdf?__blob=publicationFile
- University of Montreal ‘World Bank draws on expertise of Université de Montréal’s Cyberjustice Laboratory’ (2013). http://www.nouvelles.umontreal.ca/udem-news/news/20130211-world-bank-draws-on-expertise-of-universite-de-montreals-cyberjustice-laboratory.html

**Jurisprudence**

- European Court for Human Rights (ECtHR), *Case Yildirim v.Turkey,* 18 December 2012.
- European Court for Human Rights (ECtHR), *Case Delfi As v. Estonia,* 10 October 2013.
- Supreme Court of Costa Rica, Res. Nº 2010012790, 30 July 2010.