POLICY BRIEF | No. 1 June 2017

Center on Governance through Human Rights

Cyber Justice

Dr. Anja Mihr

Program Director, Center on Governance through Human Rights

Justice in Cyberspace

The HUMBOLDT-VIADRINA Center on Governance through Human Rights fosters the idea of Cyber Justice as an approach for defining how good governance and human rights norms can be guiding principles to govern the Internet (Mihr 2017). Cyberspace is a borderless public space in which the Internet is a network and a tool that allows different digital devices to connect and communicate. Cyberspace todays is seen as 'one-space' in which we move, work and conduct private as well as public business at the same time. But the main difference between the offline and online space and the world we live and work in is that the online-cyberspace lacks justifiability and liability of actors and institutions that provide the online-services we use. There are no digital borders, no governments, no police or tax-authorities that would globally govern all Internet users by the same principles and benchmarks.

Whereas there is no longer a controversy whether international human rights norms and standards are valid norms offline as well as online, today's controversy is about the way, the means and the litigability of these norms and standards when using the Internet and the services it provides, i.e. social media, online banking, data storage and transfer. The question of Cyber Justice is thus *who* should be held accountable and *how* in a borderless 'space' that does not yet posses any democratic governance regime as we know it from territorial and statehood based countries?

Thus far, the cyberspace is a space without globally agreed enforceable rules or governance bodies. Instead, it lacks legislative or judiciary bodies equally accessible for all, such as a cyber court and government, a bureaucracy, a police or parliament that would manage people's activities within that space globally and protect users rights and entitlements. That is why Cyber Justice is more pivotal than ever, because it aims to protect people's privacy and at the same time to enhance its human rights to participate and interact freely by means of the Internet in cyberspace.

Worldwide these challenges are well acknowledged and various international and national governmental and non-governmental approaches aim to develop a

form of 'Internet governance' or 'Cyber governance' and other forms or regulating and governing this space. The United Nations (UN), for example, along with other regional intergovernmental organizations such as the Council of Europe, the European Union (EU) or the Organization for American States (OAS), the NATO, the G7 and G20, the Shanghai Cooperation Organization (SCO), the ASEAN Regional Forum (ARF), the BRICS and the African Union (AU) have undertaken various efforts to use international and domestic governmental tools to regulate the cyberspace. They acknowledge that one state or a group of governments alone can neither regulate nor protect our privacy and rights in cyberspace sufficiently. Cyber Justice is thus still far from being achieved.

Albeit court decisions by the Interamerican Court of Human Rights, the Court of Justice for the European Union or the European Court of Human Rights over the past years have established case law that could lead to a future global judiciary for all four billion 'cyber citizens'. Yet, these regional but international court decisions are far from being globally implemented or monitored, because there is not one state or one particular actor, such as Facebook or Google, that can protect data and safeguard our human rights. For example charging Google Europe for deleting personal information about one specific person from its search profile, will still allow Internet users in other parts of the world to access the same information and data of that person elsewhere outside Europe. The claim for the 'right to forget' soon became the 'right to have ones privacy protected'. However it cannot be safguarded fully without full accordance of rules and regulations in a global level. The judgments and decisions on whether to keep our data private does not yet have any defined responsibilities. Sometimes it is governmental institutions such as Security Agencies, sometimes private companies or social media chanels such as YouTube or WhatsApp that sell and disseminate our data without our prior consent.

Generally speaking the limits of 'free floating data ' and the harm it can do to people's personal lives and their developments is not fully investigated yet. The intransparency of algorithms and the breach of data without the full-informed consent by the owner is a violation of human rights in many aspects: the human rights to privacy, to information, to movement, to development, to security and safety and even to physical integrity in case of widespread hate speech and cyber mobbing.

Good Governance in Cyberspace

Since the Internet has been left in the hands of commerical enterprises and platforms, good governance in cyberspace is about the question on how to bring governments back in and to make cyberspace a public space that ought to be governed by principles of more transparency, accountability and participation? The Internet Governance Forum (IGF) under the United Nations (UN) is one of many global initiatives and fora, in which its stakeholders aim to define a possible future Internet governance regime. The increase of mobile devices and Internet Protocols (IP) addresses in the Global South

increases the pressure to find ways and means to regulate and govern the Internet.

Today's mass labor or refugee migration would not be possible without the Internet and the organizations, orientation and communication services it provides. 'Platform economy' is a globally rising economic factor. It is a working space and precarious labor sector in which millions of people work without health insurance or any safety net and protection for their families and personal wellbeing. For example, IPv6 aims to bring some control in this sector. It is an association that sells and provides new IP addresses particularly in the Global South, knowing that the next generation of cyber citizens is standing in line (World IPV6 Launch 2016). The difference to the previous generation of IPv4 addresses is that IPv6 is better traceable and no longer anonymous. Thus, data of platform economy providers, such as Uber or MyTaxi, are easier to trace back, and so are their labor forces. This is pivotal for the growing cyber public policy sector, in which millions of companies and labor forces remain untaxed, but also unprotected.

Thus, in future, individual users and people who provide services, labor or post data in the Internet will be easier to identify and hold accountable for wrongdoings in cyberspace and misuse of data than in present times. Even though new IP addresses are mostly distributed in countries of the Global South, where there is little or no rule of law, a lack of independent judiciary and instead a poor record of human rights; it allows for the assumption, that Internet users in the Global South still lack fundamental protection of their rights and possibilities. If there is no democratic governance regime established, either offline or online, the breach of data will continue and Internet users will loose trust in services and online companies as fast as they have gained access to them in the first place. Online companies or private hackers who misuse private data for commercial or criminal interests can do so without fearing much of governmental or international control and repercussions.

In 2016 the Council of Europe launched the Net-neutrality guidelines of compulsory indications for its 47 members states ranging from Portugal to Russia, from Turkey to Iceland. Although this guideline only has a regional impact, it clearly defines the responsibilities in the struggle for who is responsible to provide best and neutral access to cyberspace, which are governments, not private corporates such as Google or Amazon. It states that 'national authorities should monitor and issue public reports on Internet traffic management practices' and that Internet traffic should be treated equally, without discrimination, restriction or interference irrespective of the sender, receiver, content, application, service or device (Council of Europe, Directorate of Communication 2016).

Neutral Internet

How important access to neutral Internet and Net-neutrality is in current developments is illustrated by the University of Konstanz in Germany and the Swiss Federal Institute of Technology, ETH, in

Center on Governance through Human Rights

Zurich. Researchers looked at 118 countries and addressed around 500 different ethnic, indigenous and marginalized communities who were excluded or discriminated to have free and neutral access to the Internet due to their remote location, their income or social status. The result was, that these communities depend to a large extend on commercial private service providers, such as Facebook or YouTube to transport their message. In highly political sensitive matters they have no other option but to put their faith in the hands of companies, that are more interested in the group's data footprints than their political cause. At the same time, the group's main resource to mobilize their communities to participate in shaping public policies in order to change their situation is the Internet. But even if their leaders and spokespersons have access to the Internet, their constituency does not necessarily have it. Thus, these political or marginalized groups are often excluded from the promise of 'full participation' and 'voices to be heard' that the Internet once made. It was seen as the 'promised tool' to free and emancipate those that have been far too long marginalized because of their ethnicity, gender, income, disability, geography or for other criteria (BETA 2016, p. 904).

As early as in 1988, the first debates about the level of accountability and neutrality of services and providers in the Internet were held. At a time when less than one percent of the world's population understood the term Internet, enterpreneurs of the Cyber World were already claiming that the 'resource used in the Internet architectures must be an accountable one'. This means whoever uses or provides information or data, services or networks on the Internet and in cyberspace must be held accountable for her or his postings (Clark 1988, p. 107). The anticipated problems became more than true in 2013 when whistleblowers such as Edward Snowdon leaked military and other intelligence information to the wider public. How to govern, regulate, control and monitor sensitive and private data in cyberspace came on to all national and international agendas. But among others, programming and the 'management of algorithem' and their role of how to protect or breach our data came to light. It soon became clear, that Internet governance, let alone Cyber Justice, ought to include the way in which algorithms are made transparenct, their programmes or providers are held accountable and how users can participate and interact with both private companies and governmental agencies when their rights are violated.

Thus the development of IT tools along with political, ethical and moral criteria for the management of data in the context of a multi administration-level on global, national or enterprise level will be as pivotal as they were in the early days of the Internet (Clark 1988, p. 113).

Human Rights in Cyberspace

International human rights norms and standards, as defined by the UN and other regional human rights regimes and their definitions of freedom, security and political participation are universal standards that are valid offline as well as online. The same has been true for good governance norms and

rules such as the question about accountability, transparency and interaction among those who use the Internet and those who manage and provide Internet services. One of the major challenges in this area is how to establish, increase or leverage public 'user' trust in the Internet and its various service providing agencies. Internet users behavior adapt to the pitfalls and challenges of the Internet. Once the confidence and trust in certain providers or telecommunication companies is lost, it is difficult to restore. Internet users often react with self-censorship or by not tapping onlines services or platforms, that could be important for their professional and personal development and wellbeing, such as health, transportation, education and media platforms. The same is true for human rights defenders (HRD) such as lawyers, teachers, social workers, judges, CSOs and so on, whose portals and comments in the Internet are sometimes the only form of protest against offline and online human rights violation and supression. But their space of intervention is shrinking with the possibilities security agencies and governments have, in tracing HRD back via their use of Internet platforms (Mihr 2016).

How to regulate, govern or judge misconduct, shrinking cyberspace or breach of data in the Internet remains the main challenge for the future. One step to bridge the many gaps between offline and online justice is the 'do-no-harm rule' that is globally accepted as a principle to manouver, negotiate and balance rights, entitlements and, last but not least to judge, what is just, adequate or an violent behavior online? The rule set limits to both, the freedom and privacy we enjoy in cyberspace. It derives from the maxim that any speech can become hate-speech, any private data can become public, if the conditions and contexts change. And this is what happens when the Internet is used to transport information, messages or commerce. All data becomes global in a matter of seconds and thus the cultural, commercial, moral or ethical contexts in which our data speed in the data highway change constantly and are difficult to manouver. This maxim of the 'do-no-harm rule' serves as a benchmark for many judges in particular at international courts and tribunals.

Generally speaking neither our freedoms nor our privacy is violated if actions on the Internet do not lead or call to any physical harm or the integrity of a person, company or a group's reputation. Nevertheless, the way we interpret 'harm', 'personal integrity' and how we understand freedom of expression, information or privacy has dramatically changed in the context of cyber space and the internet. People suffer harm because of a 'funny' posting in social media that eventually leads to loosing credibility, jobs and partnership. Thus, the way 'harm' is conducted and perceived will be pivotal for defining Cyber Justice and as such the wellbeing of the whole Internet-community.

Art 19 of the UN International Convention on Civil and Political Rights (ICCPR) on freedom of expression is seen in the context of not harming others. If free speech threatens 'public order' or the 'rights of others', their equality or right to non-discrimination, then free speech can be limited. However, the fact that 'public order' is often subject to political interpretation does not make it easier to

balance freedom against our human right to safety and security. The threshold of when free and independent conscious of mind, thought and expressed opinion turns into harm of others depends on the severity of its intent, content, public extent, imminence, likelihood of probable action and context in which it is expressed (Article 19 Global Campaign for Free Expression 2010). In some context an expression can be funny and harmless, in a different context the same expression can turn to hate crime and massive bodily harm of others.

Nevertheless, WikiLeaks or whistleblowers, let alone Facebook or Weibo cannot be considered harmful per se if they disclose 'confidential' material or hate speech to the public. It is a matter of balancing entitlements and potential harm. The tools and means the Internet provides in cyberspace do not change the principles of harms or human rights, but they urge us to renegotiate digital-borders due to the magnitude, dimensions, speed and paste that allows our expressions, images or otherwise private data to reach unwillingful or intentional a global audience that might not be anticipated in the first place. We will change our mode by which we morally judge disclosures, use postings and announcements. That is often described as Internet-literacy, too. We will become more sensitive to these postings because we have learned the negative consequence of supposingly 'funny' postings. Internet literacy will not fundamentally change our morals by which we judge and decide, but the way we think about the dimensions and magnitudes of the possible consequences our postings of news or sharing of Credit Card numbers can have.

Even the human rights to development, women, children and minority rights are under scrutiny. Because marginalized groups become even more marginalized through acts of discrimination, geoblocking or hate-speech. The structure of the Internet, its pervasiveness, and the possibility it affords for anonymity have made cyberspace a playground for those who are full of anger, prejudice and hatred and wish to spread harmful propaganda and incite hatredand violence. A quick check on any search engine provided numerous home pages that target their propaganda against immigrants, Jews, Muslims, women or homosexuals. They incite hate and encourage violence against these groups.

Thus, the 'do-no-harm' principle is the principle that makes the other rights operational and, in a sense, makes human rights universal, also in the moral discourse (Zarrehparvar 2006, p. 233).

Social Contract for the Internet

In 1996, John Perry Barlow published the first of efforts to seek a new type of social contract for the cyberspace, the 'Declaration of Independence of Cyberspace'. In this declaration he indicated the situations and controversies that today's Internet users experience on a day-to-day basis (Barlow 1996). In sixteen short paragraphs, it rebuttals that the Internet can ever be governed by private enterprises alone, and instead urges for a governmental based

Internet governace regime. In an era in which the Internet was left largely in the hands of private telecommunication companies and service providers, Barlow argues that no government had at that time the consent of the Internet users to apply arbitrary laws, censorship and restrictions to the World Wide Web. If governments would nevertheless deny such data protection and surveillange laws in accordance with the users, data will continue to be published through whistleblowers, hackers and "leakers" without the owner's consent. In other terms, the anarchy in cyberspace will not allow for the commonly known mode of governance, because the Internet requires a different form of governance as we know it from the offline world. In his prognosis Barlow assures, 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 do-no-harm rule.

Of course, reality, even cyber reality, is far from that theory, but the rule is an ideal benchmark against which users behavior can be assessed. Whether such social contract for the cyberspace will ever be realized or not, remains open. But the idea behind that is, that if there is ever a Cyber or Internet governance regime, individual responsibility and adherence to human rights will be one of the guiding principles in order to govern that space.

Latest since the UN resolution in 2013, human rights principles such as solidarity, freedom and justice are seen as a universal nexus that combines cultures, habits as well as businesses online and offline. However the way governments implement and enforce (or not) these principles varies from country to country, from domestic jurisdiction to jurisdiction. There is no universal jurisdiction when it comes to cyberspace. But it would be much needed. There is a broad agreement that freedom, justice, privacy and security are important. However, among the four billion Internet users, not everyone will have the same ideas about the realization and implementation of human rights. According to these general freedom principles and norms, a social contract for cyberspace is much discussed. Such a contract would need to be enforced by all Internet users, regardless whether they are private or public, companies or governments and so on. The heterogenity of Internet users originating from different geographical zones, linguistic areas, and cultural backgrounds leads to very different conceptions of norms and standards related to the organization of the Internet. But any decision about how to govern the cyberspace needs to be supported by a large part of the Internet community in order to ensure its effective functioning. Thus transparency and participation is fundamental in this context.

A multi- stakeholder approach enhances the information flows between the individual users, CSOs, governments and providers allows the public to form an opinion and participate in negotiations. But consensus building which includes all interested parties and creates the opportunity to make decisions, is more pivotal in the cyberspace than ever before in any offline world (Weber and Weber 2008).

A code of conduct is the basis for a social contract and subsequently the concept of Cyber justice. The code defines immoral

attitudes and behavior and responsibilities at the same time. Apart from global mechanisms that are needed to monitor and enforce, it would include personal and moral disguise and sanctions against those who violate human rights norms. In this vain the claim for a 'digital rights' based social contract claims to enable the free and neutral access and use of information and communication technologies (ICTs) such as computers and digital media, i.e. to information, to work, to communication, to health, to participation, to expression, to development to assemble, etc. (United Nations Human Rights Office of the High Commissioner 2013).[1]

Part of this code is found in the 2015 proclaimed UN Sustainable Development Goals (SDGs). The free and neutral access to the Internet is one of many prerequisites for development. In the so called developing world at least two billion people have access to the Internet, mostly through mobile devices. These figures are 40-times higher than ten years ago and shows the rapid – however, uncontrolled and unregulated – access to the Internet. These new cyber citizens have little or no experience with democracy or rule of law and lack fundamental access to it.

Global Development & Online Economy

Because of the interlinkage of private, commercial and public stakeholders that maneuver, govern or regulate our data on their own behalf in the Internet. The UN IGF promotes the multi-stakeholder approach, knowing that it can be a way to reach the goals by 2030. The UN highlights the conduct and that we all need to 'enhance the Global Partnership for Sustainable Development, complemented by a multi-stakeholder partnership that mobilizes and shares knowledge, expertise, technology – in particular communication technology – and financial resources, to support the achievement of the SDG and Agenda 2030' (UN General Assembly 2015).

In short, no realization without equal partnership and no development without a human righs based use of the Internet. Jeffrey Sachs, adviser to the UN, highlights the fact that without the Internet, none of these goals would ever come close to reality, in particular in the health, education or food sector. If the world wants to fight poverty, it needs tools. Such a tool is the responsible use of big-data for the benefit of all. The 'wise' use of data depends on how algorithms are programmed and data stored or generated and made transparent. The best programmed algorithms or artificial intelligence and robots by no means can replace the moral judgement of persons and our common-sense, but they can be helpful agents and tools, if used in a human rights complying way. Big-data can not only transfer knowledge to remote parts of the world, but also assess for example, massive data on climate, migration, business, epidemies, agrigulture and so on, in order to launch rapid help or investments for development (Sachs 2015).

[1] 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.

In its 2016 annual report the global Internet Society states that the breach of data, private and public, has increased to a new peak and mostly in countries with insufficient legal or political monitoring mechanisms such as uncorrupt parliaments and courts. Mistrust of users towards services providers or telecommunication companies has therefore increased in these countries. Once the Internet was seen as a source of truth and facts, now it turns towards the opposite extreme. Therefore governments as well as broadcasting and media companies and other private enterprises try to win back the trust of citizens and potential customers. At the same time, the Internet economy will no longer grow, if users do not trust that they can rely on the information provided online and that their data is not misused. Thus, not only the SDGs but also the world economy depends largely on the trust Internet users have in using Internet services. And in return these users have to be better informed and engaged in the processes on what happens to their data. User's trust will also depend on how good governance principles and human rights norms are upheld by companies and governments alike.

Modern economies cannot allow for its citizens to loose trust and to stop online-banking, online-bookings or online-shopping. Moreover also public services such as taxation, health or education depend on online participation of citizens. If billions of users would restrict their usage of the Internet within one year or so, public infrastructure, particularly in Europe and North America would collapse because many public services are only accessible online. That is why cyber security and data protection is part of the Internet governance regime today. Thus, because of the decreasing trust in service providers, the Internet Society has anticipated that the likeliness that we face a first 'cyber-economy-recession' is rather high (Internet Society 2016, pp. 16–21). Cyber attacks will increase, fraud and breach of data mostly for financial reasons will continue if regulatory and control mechanism are not installed. Users' identities in the Internet such as profiles, passwords, e-mail addresses etc., are stolen for profit, and companies whose legal business is to use entrusted data, spend more resources then ever in fighting this abuse. Thus, service providers are taking regulation in their own hands, because a global Internet governance that ought to do it, does not exist or will take time to be installed, whilst users loose trust every day. The e-commerce is loosing money and time which they could invest in their business otherwise. At least 40 million customer's credit cards numbers have been reported stolen in 2016 (Identity Force 2016). Private and intimate data of 37 million users were reported to be published online without their consent, most of these reports came from the US, where misuse is most often reported. Over a billion users might be affected by breaches of their private data.

Recommendations & Ways ahead for Cyber Justice

A social contract and global multi-stakeholder based Cyber or Internet governance regime can achieve Cyber Justice. Such governance regimes are user-centric and self-regulating through economic

and private incentives. First, globally acknowledged and agreed human rights and good governance principles support the establishment of an Internet contract that again is the basis for organized governance regimes in which different private, commercial and governmental actors govern. Secondly, Cyber Justice needs global independent monitoring and enforcement mechanisms, that are institutionalized global and multi-stakeholder mechanisms capable and legitimized to hold providers accountable regardless of their geographic location. A global Cyber Court and governance-monitoring bodies that work on rotating systems, clear guidelines, quotas and open application procedures (similar to the already existing IFG) can lead to a Cyber governance regime of truly global character. Cyber Justice embraces this Internet Governance approach and adds as a core principle the 'do-no-harm rule' as a mode to govern and regulate divergent interests and powers in cyberspace. Digital borders in which we can govern can only be established with clear guiding principles: human rights, good governance and 'do-no-harm'.

Reference List

Article 19 (2010). Global campaign for free expression. Study Paper. Article 19. https://www.article19.org. Accessed 1 December 2016.

Barlow, J. P. (1996). A Declaration of the Independence of Cyberspace. Electronic Frontier Foundation. https://www.eff.org/cyberspace-independence. Accessed 1 January 2013.

BETA (2016). Wir fordern digitale Grundrechte: Charta der digitalen Grundrechte der Europäischen Union; and: Digitale Ungleichheit, Forschung und Lehre, Nr. 10, 2016, p. 905.

Clark, D. D. (1988). The design philosophy of the DARPA internet protocols. Computer Communication Review, 18(4), 106–114.

Directorate of Communication (2016). Council of Europe issues network neutrality guidlines to protect freedom of expression and privacy: Press Release- DC003 (2016). Council of Europe. https://wcd.coe.int/ViewDoc.jsp?p=&id=2402819&direct=true. Accessed 1 January 2017.

Identity Force (2016). The Biggest Data Breaches in 2016. https://www.identityforce.com/blog/2016-data-breaches. Accessed 26 May 2017.

Internet Society (2016). Global Internet Report 2016: Mobile Evolution and Development of the Internet. http://www.internetsociety.org/globalinternetreport/2015/assets/download/IS_web.pdf. Accessed 1 January 2017.

Mihr, A. (2014). Good cyber governance, the human rights and multi-stakeholder approach. Georgetown Journal of International Affairs.

Mihr, A. (2016). Cyber Justice: Cyber-Governance through Human Rights and a Rule of Law in the Internet. US- China Law Review, David Publishing Company, 13(4), 314–336.

Mihr, A (2017). Cyber Justice, Human Rights and Good Governance for the Internet, Springer-Briefs, Springer Verlag.

Sachs, J. D. (2015). Data for Development. Project Syndicate. https://www.project-syndicate.org/commentary/sustainable-development-data-by-jeffrey-d-sachs-2015-05. Accessed 1 January 2017.

UN General Assembly (2015). Transforming our world: the 2030 Agenda for Sustainable Deveopment: A RES/70.1.

United Nations Human Rights Office of the High Commissioner (2013). Human Rights Indicators: A Guide to Measurement and Implementation. United Nations. http://www.ohchr.org/Documents/Publications/Human_rights_indicators_en.pdf. Accessed 1 January 2017.

Weber, R. H. and Weber, R. (2008). Social Contract for the Internet Community? Historical and Philosophical Theories for Inclusion of the Civil Society. GigaNet: Global Internet Governance Academic Network, Annual Symposium 2008. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2798970. Accessed 1 January 2017.

World IPV6 Launch (2016). IPV6 is the new normal. http://www.worldipv6launch.org/. Accessed 1 December 2016.

Zarrehparvar, M. (2006). A nondiscriminatory information society. In R. F. Jorgensen (Ed.), Human Rights in the Global inforamtion Society (pp. 226- 253). Cambridge, Massachusetts: MIT Presse.

HUMBOLDT-VIADRINA Governance Platform

The Center on Governance through Human Rights
is a Center of the HUMBOLDT-VIADRINA Governance Platform gGmbH.

Pariser Platz 6
D-10117 Berlin

Learn more at:

www.governance-platform.org/governancecenter/cogthr/