Internet Control: assessing China in a comparative European context

LL.M. 'Law in a European and Global Context'

Student: Maryant Nathalie Fernández Pérez
Supervisors: Professors Dr. Marie-José Garot & Dr. Matej Accetto

Brussels, 5th August 2015

ABSTRACT

China is unpopular for its policies on the Internet. However, we tend to forget that other countries and their economic actors also realise dubious practices on the Internet. This paper seeks to demonstrate the situation of human rights online in China shares common characteristics with the Internet policy of the European Union and some of its Member States. By choosing very specific examples, this paper offers a critical view of the Chinese Internet system, but also extends that criticism to certain practices in the EU. It provides different perspectives of the online environment from a human rights perspective.

ACKNOWLEDGEMENTS

I would like to express my gratitude to Ms. Marie-José Garot for her kindness and implication as a tutor for my thesis. "*To teach is to touch a life forever*". Indeed. Thank you for all your constructive comments and high-quality proofreading.

I am also thankful to Mr. Matej Accetto for his contributions to this study.

Thank you also to EDRi and its members, in particular to Mr. Joe McNamee. "Staying informed about human rights issues is the first step towards making change"[1], as Human Rights Watch argues. EDRi's work and passion to defend civil liberties in the online environment has been of great inspiration to this paper.

To my family and friends, thank you very much for your constant love and support.

All errors are my own.

[1]Cf. http://www.hrw.org/get-involved (last visited on 15th June 2014)

TABLE OF CONTENTS

LIST OF ABBREVIATIONS

ACLU	American Civil Liberties Union
ACTA	Anti-Counterfeiting Trade Agreement
ACHPR	African Commission on Human and Peoples' Rights
ASEAN	Association of Southeast Asian Nations
CSTD	UN's Commission on Science and Technology for Development
DNS	Domain Name System
DPI	Deep Packet Inspection
ECHR	European Convention of Human Rights
ECOSOC	UN's Economic and Social Council
ECtHR	European Court of Human Rights
EESC	European Economic and Social Committee
EDRi	European Digital Rights
EU	European Union
GATS	General Agreement on Trade in Services
GATT	General Agreement on Tariffs and Trade
GNI	Global Network Initiative
GOFA	Global Online Freedom Act
IANA	Internet Assigned Numbers Authority
ICANN	Internet Corporation for Assigned Names and Numbers
ICCPR	International Covenant on Civil and Political Rights
ICESCR	International Covenant on Economic, Social and Cultural Rights
ICT	Information and Communications Technology
IGF	Internet Governance Forum
IP	Intellectual Property or Internet Protocol
ISC	Internet Society of China
ISOC	The Internet Society
ISP	Internet Service Provider
ITU	International Telecommunication Union
NIC	National Intelligence Council
NSA	US National Security Agency
NTIA	National Telecommunications and Information Administration
OAS	Organisation of American States
OSCE	Organisation for Security and Co-operation in Europe
PNR	Passenger Number Record
SCO	Shanghai Cooperation Organisation
UDHR	Universal Declaration of Human Rights
UK	United Kingdom
UN	United Nations
UNESCO	United Nations Educational, Scientific and Cultural Organisation
US / USA	United States of America
VPN	Virtual Private Network
WCIT	World Conference on International Telecommunications
WGIG	Working Group on Internet Governance
WSIS	World Summit on the Information Society
WTO	World Trade Organisation

"And you shall know the truth, and the truth shall make you free."

John 8:32

INTRODUCTION

China has progressively become the country with the biggest number of netizens. It is estimated that among its 1.357-billion population,[2] China has more than 641 million Internet users,[3] which represents almost the triple of the figure of the second country with most users, the United States. If we consider that the Chinese population is four times bigger than the North American population, one can realise China's potential.[4] In fact, a study conducted by Microsoft shows that by 2025, 1.1 billion Chinese users will have access to the Internet, a figure which almost represents almost its entire population. Taking into account the worldwide number of Internet users expected by 2025 (4.7 billion), it is an impressive figure. Yet, Chinese people are not expected to be the only predominant population online. By 2025, 75% of Internet users will come from emerging countries, the study adds.[5]

Due to the large number of Internet users China has, and is expected to have in the coming years, it is no surprise that the Chinese government conceives the Internet as a source of development for the economy and society; a tool to modernise, reform the country and open-up its frontiers. Furthermore, the government recognises that the

[2] The World Bank, *China,* available at http://data.worldbank.org/country/china (last visited on 19th October 2014)

[3] Nevertheless, "only just over 40 percent of individuals use the Internet on a regular basis and there are only 13 fixed broadband Internet subscriptions for every 100 people. (…). Mobile broadband Internet has registered more substantial growth, but its penetration is still low, with 17 subscriptions per 100 population." Cf. Bilbao-Osorio, B., Dutta, S. and Lanvin, B. (Edrs.), *The Global Information Technology Report 2014 Rewards and Risks of Big Data*, Insight Report - World Economic Forum and INSEAD, 2014, p. 23, available at http://www3.weforum.org/docs/WEF_GlobalInformationTechnology_Report_2014.pdf (last visited on 25th April 2014).

[4] Data extracted from Internet Live Stats, *Internet Users by Country*, July 2014, available at http://www.internetlivestats.com/internet-users-by-country/ (last visited on 19th October 2014).

[5] Microsoft, *Cyberspace 2025: Today's Decisions, Tomorrow's Terrain*, June 2014, pp. 3-4, available at http://www.google.be/url?sa=t&rct=j&q=&esrc=s&source=web&cd=2&ved=0CCUQFjAB&url=http%3A%2F%2Fdownload.microsoft.com%2Fdownload%2FC%2F7%2F7%2FC7775937-748E-4E95-85FB-24581F16B588%2FCyberspace%25202025%2520Today%25E2%2580%2599s%2520Decisions%2C%2520Tomorrow%25E2%2580%2599s%2520Terrain.pdf&ei=T8SjU_-dKYW4O6CtgdAG&usg=AFQjCNH1bX4VsVzi0V9j62J2XrzdHzn78A&bvm=bv.69411363,d.ZWU (last visited on 20th June 2014).

Internet serves as a way to promote the government itself. These reasons explain why China has made a huge investment to build 8,267 million km of Internet infrastructure.[6]

In line with its predominant political direction, China has enacted an extensive set of norms in order to regulate the Internet.[7] The purported view of the Chinese government is to bring forth Internet legal and ethical education, maintain public order and security, protect minors and Intellectual Property (IP) rights, among other priorities. Chinese legislation covers regulations on *inter alia* Internet administration; security; data protection; state secrets; the ban on dissemination of sensitive information which may compromise state power, national harmony and unity, its honour, collective, social or state interests, the freedom or rights of other citizens; heresy, pornography, violence or terror. Put simply, the government's vision includes setting up limits to the freedoms and human rights online of the Chinese citizens.

Many scholars, public and private entities, civil society and human rights activists from around the world have criticised and still criticise China because of its Internet policies, its media and legal and political framework. Nevertheless, China is not the only country that has been or can be subject to criticism.

This paper defends the thesis that there are some similarities between European countries and China when designing and implementing Internet-related policies. In particular, the present paper shows some European countries set up very similar grounds used by the Chinese government for restricting fundamental rights and freedoms online.

---

[6] Information Office of the State Council of the People's Republic of China, *White Paper* on the *Internet in China*, Beijing, 8 June 2010, available at http://www.china.org.cn/government/whitepaper/node_7093508.htm (last visited on 25th April 2014)

[7] As evidenced by the abovementioned White Paper, *Op. cit*., "[s]ince 1994 China has enacted a series of laws and regulations concerning Internet administration, including the Decision of the National People's Congress Standing Committee on Guarding Electronic Signatures, Regulations on Telecommunications of the People's Republic of China, Measures on the Administration of Internet Information Services, Regulations on the Protection of Computer Information System Security of the People's Republic of China, Regulations on the Protection of the Right to Online Dissemination of Information, Provisions on the Administration of Foreign-funded Telecommunications Enterprises, Measures on the Administration of Security Protection of the International Networking of Computer Information Networks, Provisions on the Administration of Internet News Information Services, and Provisions on the Administration of Electronic Bulletin Services via the Internet, among others." "Relevant provisions of the Criminal Law of the People's Republic of China, General Principles of the Civil Law of the People's Republic of China, Copyright Law of the People's Republic of China, Law of the People's Republic of China on the Protection of Minors, Law of the People's Republic of China on Punishments in Public Order and Security Administration and other laws are applicable in the case of Internet administration".

However, this paper is not a comparative study between China the EU and/or its Member states. Instead, this paper selects examples to respond to the following research question:

Are human rights online in China restricted in a similar way than in some EU Member States?

By referring to concrete examples in several Member States of the European Union[8], this paper strives to demonstrate that some practices conducted in China restricting human rights and fundamental freedoms online are sometimes conducted within the EU as well. In fact, some online practices in the context of the European Union can be put into question from the perspective of human rights, fundamental freedoms and the rule of law.

We are of the opinion that a comparative study is not very plausible, since China's Internet policy is not comparable to the situation in the EU or any of its Member States. What this thesis tries to demonstrate is that although the EU area has a human rights protection framework, there are various similarities on the Internet between China and the EU. Our reasoning is fourfold:

First, the Internet **governance** model pursued by China is different from the one defended by the European Union and its Member States, being the latter more open to the concept of 'multistakeholderism'. One could therefore believe that the approaches to restrictions on human rights and fundamental freedoms are different in both sides. However, some instances show that this is not always the case within the EU.

Second, when addressing the **control** mechanisms exercised in some EU countries to restrict access to the Internet and/or to its content, one can acknowledge the existence of resemblances with China. We develop some of them in this paper.

Third, protection of **human rights online** and the right to obtaining **effective remedies** within the EU cannot be compared to the protection and remedies offered in practice in China. Yet, several examples happening within the EU show online restrictions to

[8] We provide examples occurring in the United Kingdom (UK), France, Spain, Estonia or Austria.

fundamental rights and freedoms fall outside the rule of law – to the detriment of Internet users.

On the Internet, online **intermediaries** play an important role, which leads us to our fourth and final point. In both the EU and China, Internet companies have progressively been conferred the power to police the Internet so as to pursue legitimate public policy objectives. Nevertheless, available evidence confirms the tendency of companies restricting human rights online without a clear, predictable or proportionate counterbalancing obligation not to act in an arbitrary way. In fact, private entities are not abiding by the positive human rights obligations that States must respect, which risk conflicting with businesses' right to conduct business freely.

In order to demonstrate the abovementioned hypothesis, we structured this paper into four chapters and a conclusion.

The **first chapter** provides an overview of the Internet governance models available and the ones defended by China and the EU, respectively. The EU considers the Internet should be governed in a different way than China. However, we point out flaws in both positions, which clearly affects the approach towards human rights online of each party. Therefore, this chapter sets up the basis for discussion.

The **second chapter** explores the different forms of Internet control in both parties. It first explains how the internet works in terms of access and content. The second chapter addresses the forms of Internet control in China and how that affects Internet users' access to the Internet and to its content in China. After exploring the Chinese situation, we demonstrate EU countries also adopt several methods of control and therefore restrict freedom of communication in certain instances.

The **third chapter** explores the human rights online situation in both China and the European Union. In particular, it focuses on the restrictions to freedom of expression and the right to privacy as well as the different ways for Internet users to obtain redress.

Before reaching a **conclusion** in **chapter five**, the **fourth chapter** discusses how the Internet can be used as a means of control in order to achieve public policy objectives,

such as national security or child protection, and explains the important role that online intermediaries play in that regard.

I. INTERNET GOVERNANCE

In order to explore the human rights situation within China and some EU countries, the first thing one needs to understand is how the Internet is governed from the perspective of both parties. This chapter first explores the Internet governance models available, mainly 'interstate participation' and 'multistakeholderism'. Secondly, it provides a critical review of both models. This will allow the reader not only to understand the differences of the Chinese approach and the EU approach (and therefore, EU countries in general), but also the main concerns about each model. Finally, this chapter provides the reader with hints on the possible future of Internet governance in order to frame the human rights discussions in each party both at present and in the future.

But what is Internet governance?

There is no consensus among scholars, civil society, the technical community, industry stakeholders or governments on the definition of Internet governance. The Working Group on Internet Governance set up by the Secretary-General of the United Nations[9] in December 2003 attempted to define it as the "development and application by Governments, the private sector and civil society, in their respective roles, of shared principles, norms, rules, decision-making procedures, and programmes that shape the evolution and use of the Internet".[10] Conversely, scholars like researcher Julien Nocetti consider that the meaning of the word "governance" guides the discussions around the topic in different directions. According to Nocetti, whereas the French expression "*governance de l'internet*" seems to refer to an external element that influences the Internet, the English version "Internet governance" refers to the specific ways in which the Internet is governed.[11] For the purposes of this paper, we follow the English

[9] WGIG, *Report of the Working Group on Internet Governance*, June 2005, p.3, available at http://www.wgig.org/docs/WGIGREPORT.pdf (last visited on 12th May 2015).
[10] *Ibid*, p. 4.
[11] Institut Français des Relations Internationales (Nocetti, J., coord.), *Internet: une gouvernance inachevée*, Politique étrangère, n° 4, hiver 2014-2015, p.10.

language expression and the WGIG's definition[12]. We further examine the technical aspects of the Internet and its management in Chapter two.

1. Models of Internet governance

The discussion on what we should consider as the most adequate model to run the Internet dates back to the end of the 90s, when the Internet Corporation for Assigned Names and Numbers (ICANN) was created – an organisation that we will describe later on. Traditionally, international law provided governance solutions solely involving States. Through a certain degree of cooperation and interaction, States reach agreements at regional or international level. This is the model that China has adopted at a global level. More recently, another type of Internet governance has gained wider acceptance. It is a model that claims to involve virtually all Internet actors. This model is often called "multistakeholderism" and has been officially endorsed by the European Union. For the purposes of this paper,[13] we thus regroup the Internet governance models into two, the interstate model and multistakeholderism.

The **first** type of Internet governance model is the '**intestate model**', according to which States gather together to provide the principles and roadmap to govern the Internet. As previously stated, China encourages this type of model, as it considers the Internet should remain under the sovereignty of each country. In the international arena, China praises the United Nations (UN) for the role it plays on the Internet. China "supports the establishment of an *authoritative* and just international administration organisation under the UN system". At the same time, it emphasises that the process shall be globally done in a *democratic* way (emphasis added). China is therefore a country that is vastly represented at the World Summit on the Information Society (WSIS), as the Information Office of the State Council of the People's Republic of China referred to in its 2010 White paper on the Internet. [14]

[12] Definition included in the Tunis Agenda of the World Summit on the Information Society. Cf. WSIS, *Tunis Agenda for the Information Society*, WSIS-05/TUNIS/DOC/6(Rev. 1)-E, 18th November 2005, paragraphs 33 and 34, available at http://www.itu.int/wsis/docs2/tunis/off/6rev1.html (last visited on 26th May 2015).
[13] We omit references to other Internet governance models, e.g. the auto-regulation model, in which the Internet would be governed by the market itself or by a technical or scientific community. See, for instance, Institut Français des Relations Internationales (Nocetti, J., coord.), *Op. cit*.
[14] Information Office of the State Council of the People's Republic of China, *Op. cit.*

The WSIS was established by the UN General Assembly Resolution 56/183 of 21st December 2001, following ITU's Resolution of 1998.[15] The WSIS was organised by the International Telecommunication Union (ITU), a specialised UN agency, with the view to discussing "the implications of the emerging information society." [16] The WSIS had two phases. The first one was held in Geneva on 10-12 December 2003, as a result of which a Declaration of Principles and a Plan of Action were adopted. The second phase took place at Tunis on 16-18 November 2005. The so-called 'Tunis Commitment' and its Agenda included Internet governance among its topics, documents which prepared the ground for an implementation and follow-up plan. Throughout those two phases, the ITU was assisted by a high-level committee and a preparatory committee, in which China took part. The function of the latter was to discuss textual proposals before they were addressed at each stage of the WSIS. [17]

Ultimately, WSIS' main goal was to purportedly build an inclusive Information Society.[18] However, the WSIS did not follow a very democratic process. Initially, it was designed for high-level representatives of the States. Later on, a multistakeholder approach was introduced. Nonetheless, stakeholders only acquired the status of observers, so they did not have the power to decide. Yet, criticism mainly expressed by civil society regarding WSIS relates to its main organiser, the ITU. First, although established by international law (at UN level), the ITU only issues recommendations. Secondly, it is highly criticised for following a top-down system in which participation is subject to membership fees[19] and stakeholders are not given much of a say because intergovernmental views are imposed, since it is a centralised system. Thirdly, ITU is accused of being largely influenced by the US.[20]

---

[15] ITU, *Resolution 73 of the ITU Plenipotentiary Conference*, Minneapolis, 1998, available at http://www.itu.int/wsis/docs/background/resolutions/73.html (last visited on 26th May 2015).
[16] Internet Society, *Understanding the WSIS+10 Review Process, The UN and its 10-year Review of the WSIS in December 2015*, May 2015, available at https://www.internetsociety.org/sites/default/files/WSISplus10-Overview.pdf (last visited on 26th May 2015).
[17] See ITU, *Basic Information - Frequently asked questions*, available at http://www.itu.int/wsis/basic/faqs.asp (last visited on 12th February 2015).
[18] Internet Society, *Op. Cit.*
[19] ITU, *Membership*, available at https://www.itu.int/en/about/Pages/membership.aspx (last visited on 15th February 2015).
[20] Masnick, M., *Tell The UN To Keep Its Hands Off The People's Internet,* 1st June 2012, available at https://www.techdirt.com/articles/20120601/10182719172/tell-un-to-keep-its-hands-off-peoples-Internet.shtml (last visited on 17th June 2014).

The goals set as a result of the WSIS were scheduled to be reviewed in December 2015 through the so-called "WSIS+10" process. In fact, "the Tunis Agenda called upon the UN General Assembly [to] conduct an overall review of the implementation of WSIS outcomes in 2015".[21] Throughout the WSIS action plan and implementation, the ITU collaborated with the United Nations Educational, Scientific and Cultural Organisation (UNESCO) and other UN bodies, such as the UN's Economic and Social Council (ECOSOC) or the UN's Commission on Science and Technology for Development (CSTD).[22]

As expressed at the beginning of this chapter, **the obvious example of the interstate model is China**. According to China's Internet vision, nations are the sole sovereign authorities to establish what triggers Internet security and responses. Different visions ought to be respected and, in order to comply with international practices, countries need to cooperate and collaborate within the international arena. Pursuant to the Chinese government's views, China collaborates and cooperates with other countries. In other words, China welcomes interstate participation to govern the Internet on an international, regional or a multilateral basis, through *inter alia* the WSIS (and WSIS+10), the ASEAN or the Shanghai Cooperation Organisation (SCO). For instance, in 2010 China is reported to have sent representatives to international meetings and set up delegations in more than 40 countries to observe and learn from them. Additionally, China recognised having entered into bilateral agreements with countries like the US, the UK, Germany, Italy, Hong Kong[23] or with Russia. In the latter case, for example, Russia and China entered into a cybersecurity agreement on 30 April 2015,[24] which builds upon previous alliances in the Internet world.[25]

---

[21] Brown, D., and Kaspar, L., *Everything you need to know about the WSIS+10 review*, Association for Progressive Communications News, 28th January 2015, available at https://www.apc.org/en/news/everything-you-need-know-about-wsis10-review (last visited on 26th May 2015).
[22] Internet Society, *Op. cit.*
[23] Information Office of the State Council of the People's Republic of China, *Op. cit.*
[24] Kulicova, A., *China-Russia cyber-security pact: Should the US be concerned?,* Russia Direct, 21st May 2015, available at http://www.russia-direct.org/analysis/china-russia-cyber-security-pact-should-us-be-concerned (last visited on 1st June 2015).
[25] Commissioner for Human Rights, *The rule of law on the Internet and in the wider digital world*, Issue Paper, CommDH/IssuePaper(2014)1 prepared by Prof. Douwe Korff, Council of Europe, 8th December 2014, pp. 40 and 41, available at https://wcd.coe.int/com.instranet.InstraServlet?command=com.instranet.CmdBlobGet&InstranetImage=2734552&SecMode=1&DocId=2262340&Usage=2 (last visited on 1st June 2015).

In sum, while defending a state-sovereign Internet, "China has moved from rejection of international institutions to sustained, deep engagement".[26] In practice, however, China's international participation is not a synonym of respect of Internet users' human rights and fundamental freedoms. While Article 3(3) of the Russia-China cybersecurity agreement example mentioned above, commits to develop and promote international law norms to ensure national and international information security, Article 4(2) allows restrictions to the fundamental freedoms to seek, receive and disseminate information to be imposed by the legislation of the other country to ensure "national security".[27]

The **second** model of Internet governance involves the **participation of different actors.** Under the **'network of networks' model**, there is no one actor which runs the Internet. In fact, this model was proposed as an alternative to the proposals from the Internet Society (ISOC)[28] or the ITU. This model was further developed under the WSIS[29] and more recently in NETmundial and the UN Internet Governance Forum (IGF). Even the ITU made some progress in its meeting in Busan 2014. One type of the 'network of networks' model is the so-called 'multistakeholderism', which is supported by the EU and its institutions and by most civil society organisations.[30] So, because multistakeholder mechanisms have the potential to include a wide range of stakeholders; the Internet is not run by a moral or legal person, by a government or various countries. To the contrary, the Internet is or should be governed by "multistakeholders".

The principle of **multistakeholderism** implies the inclusion of the various actors in the decision-taking process. That includes all international organisations, companies, the

[26] Hachigian, N., Chen, W. and Beddor,C., *China's New Engagement in the International System. In the ring, but punching below its weight,* Center for American Progress, November 2009, p. 12, available at http://www.americanprogress.org/wp-content/uploads/issues/2009/11/pdf/chinas_new_engagement.pdf (last visited on 31st March 2014)

[27] Government of the Russian Federation, Order No. 788-p on signing the Agreement between the Government of the Russian Federation and the Government of the People's Republic of China regarding International CyberSecurity, 30th April 2015, available at http://government.ru/media/files/5AMAccs7mSlXgbff1Ua785WwMWcABDJw.pdf (last visited on 1st June 2015).

[28] For information concerning the ISOC, see http://icannwiki.com/index.php/Internet_Society (last visited on 17th June 2014).

[29] Kleinwächter, W, *Beyond ICANN Vs ITU? How WSIS Tries to Enter the New Territory of Internet Governance*, 2004 Gazette 66 (3-4): 233–51; cf. Musiani, F. and Pohle, J., *NETmundial: only a landmark event if 'Digital Cold War' rhetoric abandoned*, 27th March 2014, available at http://policyreview.info/articles/analysis/netmundial-only-landmark-event-if-digital-cold-war-rhetoric-abandoned (last visited on 17th June 2014).

[30] This model has been

civil society, the technical community, scholars, public authorities and the netizens. More precisely, an Internet run by a multistakeholder approach includes civil society; the Industry; Academia; Technical experts, but also the ICANN; the Internet Architecture Board (IAB), which deals with technical and engineering aspects of the Internet, supervising the Internet Engineering Task Force (IETF) and the Internet Research Task Force (IRTF); the IGF, whose aim is to gather global multistakeholders to discuss Internet governance issues and whose mandate, initially ending in 2015, has been subject to extension requests;[31] Governments and Inter-governmental organisations, such as the European Union, the International Organisation for Standarisation, Maintenance Agency (ISO 3166 MA), the Internet Society (ISOC), the 5th Regional Internet Registries (RIRs) or the World Wide Web Consortium (W3C); as well as Internet Network Operators' Groups.[32]

In practice, it is harder to ensure all actors are represented within the multistakeholder model. However, the criteria and the mere possibility to be present and have an influence on the decision-making process, even if the outcome is generally not binding, is remarkably different to the interstate model. In the multistakeholder model, it is essential that all actors enjoy the same level of importance or at least that the procedure respects the principle of equality.

The level of democracy within the principle of multistakeholderism has been criticised because it does not resolve the deficiencies of power structures in practice. The positive side is that if stakeholders refuse to participate, such behaviour can put the legitimacy of an initiative into question.[33] An example can be the European Commission's multistakeholder project called 'Licenses for Europe', which was dropped due to

[31] For instance, on 11th February 2015, the European Parliament adopted a Resolution (i.e. a political statement which is non-binding) *inter alia* asking for the IGF renewal at the UN General Assembly in December 2015. Cf. European Parliament, *Resolution on the renewal of the mandate of the Internet Governance Forum*, 2015/2526(RSP), 11th February 2015, available at http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P8-TA-2015-0033+0+DOC+XML+V0//EN&language=GA (last visited on 1st June 2015).

[32] ICANN, Infographic, *Who Runs the Internet?*, 2013, available at www.xplanations.com/whorunstheinternet (last visited on 2nd January 2015).

[33] IGFWatch news, *Debunking eight myths about multi-stakeholderism*, 25th April 2015, available at http://igfwatch.org/discussion-board/debunking-eight-myths-about-multi-stakeholderism (last visited on 26th April 2015).

concerns raised by several stakeholders.[34] But is multistakeholderism better than the interstate model?

2. Analysing multistakeholderism

This study argues that an appropriate multistakeholder model ought to allow the creation of models of Internet governance based on a bottom-up approach, being free, open and ensuring all actors are represented in the forums to be constructed.

In principle, there is no obvious reason to think multistakeholderism is a bad approach because it brings everybody on board. In theory, it gives stakeholders the opportunity to express their views and have the ability to have them taken into account. Evidence however shows that one of the most common problems of the multistakeholder model resides in the distribution of power. Although participation is in principle inclusive, governments or intergovernmental agencies and even corporations often play a greater role.[35] If inclusiveness is not fulfilled, negotiations may not be driven by the common good.

On 23rd and 24th April 2014, the multistakeholder approach was tested at NETmundial, the Global Multistakeholder Meeting on the Future of Internet Governance, which was held in Brazil.

Stakeholders generally had big aspirations on NETmundial as they believed it would provide a more decentralised model as compared to the WSIS; a model less dominated by the US.

The expectations on NETMundial's outcomes increased when the US Commerce Department's National Telecommunications and Information Administration (NTIA) announced[36] its desire to bring changes to the Internet Assigned Numbers Authority

[34] For more information, see, for example, EDRi, *Failure Of "Licenses For Europe",* 20th November 2013, available at https://edri.org/failure-of-licenses-for-europe/ (last visited on 26th April 2015).
[35] See principle nine of EDRi's Digital Rights Charter https://www.wepromise.eu/en/page/charter (last visited on 17th June 2014).
[36] See http://www.Internetgovernance.org/wordpress/wp-content/uploads/2014-03-ICANN-IANA-Role-Structures.pdf (last visited on 17th June 2014).

(IANA) function and the debate on ICANN.[37] In this sense, NETmundial appeared as a transition of the ICANN and the IANA situation.[38]

ICANN is an organisation which mainly manages and coordinates three functions. First, the domain names available on the Internet –what is called the "Domain Name System" (DNS)–. Second, Internet Protocol (IP) addresses. Third, protocol port and parameter numbers. Having its main offices in Los Angeles, Singapore and Istanbul, it has several engagement centres, including Beijing and Brussels'.[39] For its part, IANA "is responsible for global coordination of the Internet Protocol addressing systems, as well as the Autonomous System Numbers used for routing Internet traffic."[40] IANA was configured as a department of the ICANN. Nonetheless, on 14th March 2014 the U.S. Commerce Department's National Telecommunications and Information Administration (NTIA) announced its intention to transition IANA to "the global multistakeholder community", so the contract with ICANN would expire[41] in September 2015, with a margin of manoeuvre of at least two extra years.

From an EU perspective, the European Commission welcomed the transition[42], as it had previously declared.[43] On 10th June 2014, the former Vice-president of the European Commission, Ms. Neelie Kroes, expressed a more nuanced view at the WSIS

[37] Wagner, B., *Calling a Bluff? Internet Governance Poker Heats up*, 9th April 2014, available at http://cgcsblog.asc.upenn.edu/2014/04/09/calling-a-bluff-Internet-governanhttps://www.iana.orgce-poker-heats-up/?utm_source=feedburner&utm_medium=email&utm_campaign=Feed:+CGCSMediaWire+%28The+Center+for+Global+Communication+Studies+%28CGCS%29%29 (last visited on 17th June 2014).

[38] DomainNewsAfrica, *A transition to decentralized Internet, but will we get there by 2015?,* 27th March 2014, available at http://domainnewsafrica.com/a-transition-to-decentralized-Internet-but-will-we-get-there-by-2015/ (last visited on 17th June 2014).

[39] For more information, see Zalnieriute, M. and Schneider, T., *ICANN's procedures and policies in the light of human rights, fundamental freedoms and democratic values*, Expert Report for the Council of Europe, DGI(2014)12, 16 June 2014, available at http://www.coe.int/t/dghl/standardsetting/dataprotection/TPD_documents/ICANN-PoliciesProcedures%2816June2014%29.pdf (last visited on 4th December 2014).

[40] IANA, *Number resources*, available at https://www.iana.org/numbers (last visited on 2nd June 2015).

[41] NTIA, *NTIA Announces Intent to Transition Key Internet Domain Name Functions,* 14th March 2014, available at http://www.ntia.doc.gov/press-release/2014/ntia-announces-intent-transition-key-internet-domain-name-functions (last visited on 20th June 2014)

[42] European Commission, *Towards further Globalisation of the Internet*, Press release, 15th March 2014, available at http://europa.eu/rapid/press-release_STATEMENT-14-70_en.htm (last visited on 20th June 2014)

[43] E.g. In the Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on *the Internet Policy and Governance Europe's role in shaping the future of Internet Governance*, COM/2014/072 final, 12th February 2014, available at http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52014DC0072&from=EN (last visited on 20th June 2014).

in Geneva. In fact, she welcomed the USA's decision to "transition core Internet functions for more open management and stronger accountability", but seemed more sceptical about its follow-up. According to the European Commission, the Internet shall be inclusive in the sense of including developing countries.[44] Moreover, former Commissioner Neelie Kroes qualified the Internet as being open, unified and global and urged for its governance to be "[o]pen and transparent, global and multi-stakeholder".[45] Such qualifiers go along with the European Parliament's view of the Internet as "a global public good". Its "governance should be exercised in the common interest", from the perspective of the Parliament.[46]

As for NETMundial in particular, the European Commission welcomed the outcome of the Brazilian meeting[47] even though experts considered this should not be the case because one of the main policy demands of Commissioner Kroes in NETmundial was the exclusion of intermediary liability from the final document and the essence of this demand was not respected.[48]

From a Chinese perspective, multistakeholderism is not considered to be an adequate approach. In fact, China replied to the public consultation carried out at NETmundial, rejecting multistakeholderism and reinforcing its sovereign position over the Internet. This approach was already presented in December 2012, at the World Conference on International Telecommunications (WCIT). [49] The ITU organised the WCIT, which was categorised by the press as a confrontation between two visions in Internet governance.[50]

---

[44] It is important that developing countries further engage in the Internet governance discussions. In fact, it is estimated that in 2025 nearly 69% of people in emerging economies will be using the Internet. If we take into account that in developed countries that percentage increases up to 91% of the population, "internet dependence will not just be a concept, but rather the new reality", as evidenced by a recent report of Microsoft on the future of cyberspace. Cf. Microsoft, *Cyberspace 2025…Op. cit.*, p. 2.

[45] European Commission, *Inclusive governance for a global Internet*, press release (speech), 10th June 2014, available at http://europa.eu/rapid/press-release_SPEECH-14-447_en.htm (last visited on 20th June 2014).

[46] European Parliament, *Resolution on internet governance: the next steps,* (2009/2229(INI)), 15th June 2010, available at http://www.europarl.europa.eu/sides/getDoc.do?type=TA&reference=P7-TA-2010-0208&language=EN (last visited on 2nd June 2015).

[47] Kroes, N., *My thoughts on NETmundial and the Future of Internet Governance*, available at http://ec.europa.eu/commission_2010-2014/kroes/en/content/my-thoughts-netmundial-and-future-internet-governance (last visited on 11th June 2014).

[48] See for instance McNamee, J., *NETmundial…, Op. cit.*

[49] See http://www.itu.int/en/wcit-12/Pages/default.aspx (last visited on 17th June 2014).

[50] Musiani, F. and Pohle, J., *Op. cit.*; Cf. Wagner, B., *Op. Cit.*

As in the WCIT, China presented its views at NETMundial[51] together with Russia and Tajikistan and Uzbekistan.[52] In short, China defended a model in which States should remain in power. The four countries want an international voluntary code of conduct of behaviour for states with the aim of achieving international consensus. They highlighted the need of cooperation and coordination, but at the State and the UN level, as well as at the level of other international and regional organisations. The code of conduct proposed,

> "[e]ach State voluntarily subscribing to the code pledges: […] (e) To reaffirm all the rights and responsibilities of States to protect, in accordance with relevant laws and regulations, their information space and critical information infrastructure from threats, disturbance, attack and sabotage".

From our perspective, which is close to civil society, however, neither of the positions of the EU or of countries like China seem to draw the right balance. NETMundial went beyond the Tunis Agenda within the WSIS, making some progress both substantially and formally, and being more respectful as regards fundamental rights and freedoms online as compared to the Chinese proposal. However, NETMundial is not exempt from criticism, as explained below.

On the one hand, participation was important as part of the *multistakeholderism* approach. In NETMundial, all actors, whether public authorities, the industry, the technical community, civil society or users, were given the opportunity to submit their views at a first stage on Internet governance and present a roadmap for the future.[53] During the meetings in São Paolo, remote participation was possible as well. Whereas the process was deemed to be participatory, the forum missed some key contributions. According to the preamble of the final document of NETMundial, only "thousands of people"[54] provided their comments on a topic that affects the whole world.

As far as governments were concerned, for example, there was a lack of representation from African and Latin-American countries. Developing countries were greatly underrepresented. In addition, many European governments did not submit a response

[51] See the whole response at http://content.netmundial.br/contribution/international-code-of-conduct-for-information-security/67 (last visited on 17th June 2014).
[52] Musiani, F. and Pohle, J., *Op. cit.*; Cf. Wagner, B., *Op. Cit.*
[53] See the analysis conducted to ascertain the times 'multistakeholderim' appears in the different submissions received at NETmundial at http://ajantriks.github.io/netmundial/track_multistakeholder.html (last visited on 18th June 2014).
[54] As stated in the preamble of NETmundial's final document.

to the consultation, such as Portugal, Italy, Ireland or Belgium.[55] As for the private sector, most of the views on the subject came from US companies.[56] Notwithstanding the involvement of several stakeholders, some meetings were withheld from public discussions and certain meetings could not be followed remotely.

Important topics were delayed for later discussion. For instance, the outcome of the NETMundial Forum, the so-called 'NETMundial Multistakeholder Document',[57] discarded Internet management and opted to refer to Internet governance.[58] Indeed, whereas China pleaded for an Internet management system in its response to the public consultation at NETmundial, that approach was not adopted.

Traffic management is a net neutrality issue that NETMundial could have addressed, but it did not. Internet management is linked, or may be linked with traffic management. Traffic management is not wrong per se. Certain flexibility is needed in very exceptional and framed circumstances. However, traffic management measures are used as a means to discriminate on the basis of content, destination or type of data, therefore representing a violation of the most important principle of the Internet, that is, net neutrality. If arbitrarily imposed, traffic management measures on the Internet can undermine the rule of law and freedom of communication. Very sensitive topics, such as child protection may justify traffic management measures. The problem is that a valid public interest can turn into a means to filter more and not just content that does not seem 'appropriate' for children, for instance. In such a case, those measures may become disproportionate and applied in a discriminatory way.[59]

Moreover, the NETMundial Multistakeholder Document posed several problems, which could be summarised non-exhaustively as follows.

[55] See http://ajantriks.github.io/netmundial/map_no_contrib_govt.html (last visited on 18th June 2014).
[56] See the analysis conducted on the origin of the submissions divided by categories of stakeholders at http://ajantriks.github.io/netmundial/contributions_org_type.html (last visited on 18th June 2014).
[57] See the final document at http://netmundial.br/wp-content/uploads/2014/04/NETmundial-Multistakeholder-Document.pdf (last visited on 17th June 2014).
[58] Muller, M., *NETmundial moves net governance beyond WSIS*, 27th April 2014, available at http://www.Internetgovernance.org/2014/04/27/NETmundial-moves-net-governance-beyond-wsis/ (last visited on 17th June 2014).
[59] *Ibid.*

First, even if decisions were supposed to be taken by *consensus*, NETMundial reflected what happened at the 2013 ITU treaty conference in Dubai, that is, many countries joined Russia, Iran and China,[60] asking the UN to play the main role in Internet Governance. The text mentions '*consensus*' on multiple occasions referring to the way recommendations and decisions need to take place in the field of Internet governance. Nonetheless, the document nuanced 'consensus' with many adjectives, such as 'broad consensus', 'rough consensus' or consensus 'to the extent possible'. Put simply, NETMundial was not a real-consensus process.[61]

Secondly, NETMundial's final document also addressed *transparency and accountability.*

On the one hand, transparency is a great tool. It does not solely refer to being objective. Transparency is not enough by itself, indeed. For instance, there is a certain degree of transparency in China to the extent that we become aware of certain number of abuses of law or restrictions to freedom of expression. Nevertheless, if citizens cannot, or the government is not willing to, do anything meaningful to combat abuses and human rights restrictions, transparency will never be enough.

On the other hand, accountability fills the gap transparency alone cannot. Transparency without *accountability* would seem like when Google issues a transparency report informing of a government's request to shutdown content or request for users' data.[62] That is why accountability needs to be stressed in discussing measures to protect freedom of expression, freedom of communication, e-accessibility or privacy rights.[63]

To start with, publishing data is not enough. Raw data needs to be put in context. Information should be relevant and accessible at the right time (at an early stage) and be as accurate as possible. When we add accountability to that, we allow all stakeholders, from the top to the bottom, i.e. from public authorities to legal and natural persons to

[60] Genachowski, J. and Goldstein, *G.M., 'Global' Internet Governance Invites Censorship*, 3rd April 2014, available at http://online.wsj.com/news/articles/SB10001424052702303978304579471670854356630 (last visited on 18th June 2014)
[61] http://www.igovernment.in/igov/editorial/39494/consensus-netmundial (last visited on 18th June 2014).
[62] See Google, *Transparency report*, available at http://www.google.com/transparencyreport/?hl=en-GB and McNamee, J., *Google's right to be forgotten – industrial scale of misinformation*, 19th June 2014, available at http://edri.org/forgotten/ (last visited on 16th June 2014).
[63] See http://www.transparency-initiative.org/about/definitions (last visited on 13th June 2014).

respond for their actions and make available appropriate redress mechanisms. For instance, being assessed by various standards, being subject to periodic investigation, being held liable for allegedly illegal conduct and judicial redress, among others.

Fourthly, whereas NETmundial's biggest achievement is the declaration of the Internet as an open and global resource, NETMundial has been highly criticised for the use of concepts of the Anti-Counterfeiting Trade Agreement (ACTA), which was rejected *inter alia* by the European Parliament in 2012. For instance, the executive Director of the umbrella organisation European Digital Rights (EDRi), Joe McNamee, warned of the dangers of referring to '*fair process'*. According him, 'fair process' offers no guarantees, as it is neither an equivalent word for "fair trial" nor "due process", which are the concepts established under international law.[64]

3. The future of Internet governance

In the near future, Internet governance discussions are expected to take place in different fora. Following professor Kleinwächter, the near future of Internet governance could be summarised as follows:

From a technical point of view, the near future looks like it be dedicated to ascertain how the IANA will be handled by an accountable multistakeholder mechanism.

From a political point of view, the IANA contract would ideally need to transition into a multistakeholder management approach, as scheduled. Otherwise, Kleinwächter foresees that the WSIS 10+ conference would be used by some countries to plead for a "multilateral governmental oversight" instead. Also, the mandate of the Internet Governance Forum (IGF) would need to be adopted, following the 69th UN General Assembly's failure to do that.[65] In addition, as a follow up to NETMundial, the

[64] McNamee, J., *NETmundial, multistakeholderism and fair process*, 7th May 2014, available at http://edri.org/enditorial-netmundial-multistakeholderism-and-fair-process/ (last visited on 20th June 2014).
[65] Kleinwächter, W., *Internet Governance Outlook 2015: Two Processes, Many Venues, Four Baskets*, 3rd January 2015, available at http://www.circleid.com/posts/20150103_internet_governance_outlook_2015_2_processes_many_venues_4_baskets/ (last visited on 16th January 2015).

NETMundial Initiative[66] was set up and managed by the Brazilian Internet Steering Committee, the World Economic Forum or ICANN. Civil society organisations have joined forces with other organisations, such as the Just Net Coalition[67] or the World Social Forum, which is a civil society alternative to the World Economic forum.

From a policy point of view, Kleinwächter considers there should be an agenda for Internet Governance by 2025, which should include issues related to cybersecurity, cybereconomy, human rights and technology developments.[68]

II. INTERNET CONTROL

The Internet is a "global facility available to the public"[69]. From a technical point of view, that means that the Internet is "a global system of interconnected computer networks".[70] One device can communicate with another device because they all use the same language, the Internet Protocol (IP). On top of the Internet protocol, different protocols or conventions work to allow data flows. The Internet has the potential to be fully open and flexible insofar as a single language is used for all communications and content is transferred by conventions or protocols that are built on the Internet Protocol. The Internet was thus created with no limits to innovation, openness or flexibility.[71]

However, several techniques and actions are put in place in order to jeopardise the openness of the Internet. Whether by states, companies, individuals or groups of individuals, the Internet can be subject to control. Contrary to Internet governance, Internet control does not solve the question of who should or does run the Internet, but shows how the open, flexible, innovative nature of the Internet can be controlled – to the detriment of end-users and the essence of its value for society.

---

[66] https://www.netmundial.org/about (last visited on 16th January 2015).
[67] http://justnetcoalition.org (last visited on 16th January 2015).
[68] Kleinwächter, W., *Op cit.*
[69] As defined by the World Summit on the Information Society. Cf. WSIS, *Geneva Declaration of Principles,* WSIS-03/GENEVA/DOC/0004, Geneva, 10th-12th December 2003, para. 48, available at http://www.itu.int/dms_pub/itu-s/md/03/wsis/doc/S03-WSIS-DOC-0004!!PDF-E.pdf (last visited on 11th January 2015).
[70] EDRi, *How the Internet Works. A guide for policy-makers*, The EDRi papers, Issue 03, 23rd January 2012, p. 3, available at http://www.edri.org/files/2012EDRiPapers/how_the_internet_works.pdf (last visited on 12th October 2014).
[71] *Ibid*. pp. 3 and 4.

In this chapter we demonstrate how access to the Internet is the first step to have access to the full range of benefits of the Internet. Access to the Internet is often controlled and sometimes prevented not only in China, but also within the European Union. Accordingly, this chapter gives an overview of the different ways both China and the European Union or its Member states control the Internet, namely, through censorship, through the role of intermediaries and self-censorship. This overview demonstrates that within the EU, there are approaches which lead to unreasonable, unjustified and/or disproportionate approaches. Among the levels of control which can be exercised over the Internet, intermediaries play a key role.

1. Access to the Internet and to its Content.

In order to enjoy all the possibilities the Internet offers, everyone should have access to the Internet. It is the starting point. According to ITU Statistics, in 2013, 2.7 billion people used the Internet.[72] At the end of 2014, ITU reported that the Internet counted 3 billion users. What is more, the prospect for Internet user penetration is bigger because it is calculated that 4.3 billion people are not connected yet, of which 90% live in developing countries.[73] In this sense, there are differences between countries around the world,[74] including within China and the EU. The level of Internet penetration in the European Union is different to the one experimented in China.

On the other hand, the Internet "is becoming each day larger [but] more fractured", as Parfrey argues.[75] The Internet works as a human rights enhancer thanks to the principle

[72] For the purposes of the ITU 2014 report, "Internet users" "refers to people who used the Internet from any location and for any purpose, irrespective of the device and network used, in the last three months." Cf. ITU, *Measuring the Information Society Report 2014*, 24th November 2014, pp. 15 and 222, available at http://www.itu.int/en/ITU-D/Statistics/Documents/publications/mis2014/MIS2014_without_Annex_4.pdf (last visited on 5th January 2015).
[73] *Ibid*., p. 15.
[74] In recent years, price discrimination practices (such as zero rating) are having a destructive effect of restricted access. See, for instance, AccessNow, *Policy Brief: Access' position on zero rating schemes*, 2015, available at https://s3.amazonaws.com/access.3cdn.net/d812d59f706c3e8a75_w0m6iipn5.pdf (last visited on 27th July 2015).
[75] Palfrey, J. G., *Local Nets on a Global Network: Filtering and the Internet Governance Problem. THE GLOBAL FLOW OF INFORMATION*, Harvard Law School, Public Law & Legal Theory Paper Series, Working Paper No. 10-41, available at http://ssrn.com/abstract=1655006 (last visited on 31st March 2014).

of net neutrality, which is a term coined by Professor Tim Wu.[76] Net neutrality is a principle according to which every point on the network can connect to another point, without discrimination on the basis of origin, destination or type of data. In order words, internet traffic is treated equally.[77] Net neutrality is about freedom of communication, encryption, privacy and the rule of law. Non-neutrality means that we are no longer free to receive and impart the information of our choice. We would be locked into a closed environment. When we lose on net neutrality[78], we lose on our freedom to receive and particularly to impart information. But we also lose when ISPs police the Internet (as they will no longer be able to credibly claim a "mere conduit" liability exception). In this sense, voluntary measures to block or discriminate on content raise legal concerns vis-à-vis the International Covenant on Civil and Political Rights, the Charter of Fundamental Rights of the European Union[79] and the e-Privacy Directive,[80] including respect of confidentiality of communications.

In the **European Union**, authorities focus on providing EU citizens with a high-speed broadband access. Access to basic broadband was one of the first problems tackled by the EU Digital Agenda. According to the European Commission, this problem has been nearly been solved. In fact, most of the legislative proposals and policy documents adopted put their emphasis on education, capability building, access to the digital arena[81] or even on the need to include rural areas or developing countries.

As regards net neutrality, however, it has been hard for the EU to find a common ground to deliver on its political promises on net neutrality.[82] In 2013 the European

[76] Wu, T., *A proposal for Network Neutrality*, June 2002, available at http://www.timwu.org/OriginalNNProposal.pdf (last visited on 21st June 2015).
[77] EDRi, *Net neutrality*, The EDRi papers, Issue 08, 22nd December 2013, available at https://edri.org/files/paper08_netneutrality.pdf (last visited on 29th January 2015)
[78] See more information on Belli, L. and De Filippi, P. (Eds.), The Value of Network Neutrality for the Internet of Tomorrow, Report of the Dynamic Coalition on Network Neutrality, November 2013.
[79] Charter of Fundamental Rights of the European Union, available at http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:12010P&from=EN (last visited on 3rd August 2015).
[80] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector, available at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0058:en:HTML (last visited on 3rd August 2015).
[81] Fernández Pérez, M., *EC's Scoreboard 2014: Broadband access improved, challenges remain*, 4th June 2014, available at http://edri.org/ecs-scoreboard-2014-broadband-access-improved-challenges-remain/ (last visited on 17th June 2014).
[82] Fernández Pérez, M., *Net Neutrality: document pool II*, 25th April 2015, available at https://edri.org/net-neutrality-document-pool-2/ (last visited on 10th June 2015).

Commission proposed a Telecommunications Single Market Package.[83] However, the proposal contained a series of loopholes related to net neutrality. On 3rd April 2014, the European Parliament adopted a legislative resolution defending net neutrality[84].[85] However, Member States have several approaches, expressed within the Council of the European Union – the institution which represents the twenty-eight Member States. While countries like the Netherlands or Slovenia have passed laws that protect net neutrality, most EU countries do not have enough protections against discriminatory treatment of traffic.[86] On 30th June 2015, the European Parliament, the Council of the EU and the European Commission reached an agreement to regulate net neutrality.

Besides the threats against net neutrality worldwide (e.g. in India[87] or Mexico[88]), the Vice-President of the Commission, Ansip argued in his hearing before the Parliamentary committee on the Internal Market and Consumer Protection (IMCO) that "all the traffic in the Internet has to be treated equally, nobody has [the] right to abuse their dominant position in the market or gate keeper's position."[89] That should be guaranteed not only in the EU or China, but in the whole world.

[83] European Commission, Proposal for a Regulation of the European Parliament and of the Council laying down measures concerning the European single market for electronic communications and to achieve a Connected Continent, and amending Directives 2002/20/EC, 2002/21/EC, 2002/22/EC, and Regulations (EC) No 1211/2009 and (EU) No 531/2012 - COM(2013) 627 final, 11th September 2013, available at http://ec.europa.eu/digital-agenda/en/connected-continent-single-telecom-market-growth-jobs (last visited on 9th June 2015).

[84] European Parliament legislative resolution of 3rd April 2014 on the proposal for a regulation of the European Parliament and of the Council laying down measures concerning the European single market for electronic communications and to achieve a Connected Continent, and amending Directives 2002/20/EC, 2002/21/EC, 2002/22/EC, and Regulations (EC) No 1211/2009 and (EU) No 531/2012 (COM(2013)0627 – C7-0267/2013 – 2013/0309(COD)), available at http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P7-TA-2014-0281+0+DOC+XML+V0//EN (last visited on 8th June 2015).

[85] Access and EDRi, *Net neutrality – building on success*, available at https://www.accessnow.org/blog/2015/06/01/net-neutrality-building-on-success (last visited on 8th June 2015).

[86] See how the ordinary legislative process functions here: European Parliament, Legislative powers. Ordinary legislative powers, available at http://www.europarl.europa.eu/aboutparliament/en/20150201PVL00004/Legislative-powers (last visited on 9th June 2015).

[87] Cf. http://www.netneutrality.in/ (last visited on 10th June 2015).

[88] Ley Federal de Telecomunicaciones y radiodifusión, Mexico, 14 July 2014, available at http://www.diputados.gob.mx/LeyesBiblio/ref/lftr/LFTR_orig_14jul14.pdf (last visited on 8th June 2015).

[89] IMCO, Hearing of Andrus Ansip, Vice-President and Commissioner-Designate (Digital Single Market), available at http://www.elections2014.eu/resources/library/media/20141022RES75838/20141022RES75838.pdf (last visited on 10th June 2015).

For its part, **China** has injected a lot of capital into Internet infrastructure construction.[90] However, access to the Internet in China is not equally distributed throughout the country. In particular, the western and rural areas are less 'connected'.[91] What is more, statistics foresee a reduction in the willingness or capability to use the Internet, showing that such absence of motivation derives from the lack of resources, time and knowledge about IT matters, Internet unavailability and age.[92] Notwithstanding this digital gap, the Chinese government seems to be willing to boost the use of the Internet. In fact, it considers that "Internet technology lowers the cost of information – of its acquisition, storage, indexing, and distribution – to nearly zero".[93]

According to a study conducted by the Media Consulting Group for the European Parliament, "in spite of its principal role as a regulator, the State is now showing signs of becoming more involved in trying to reap financial benefit from China's Internet boom. At the end of 2008, SARFT abruptly declared that all video portals (the most profitable sector) had to become State-owned. After some negotiations, portals created before the regulation were allowed to remain private, though they are under an obligation to get a SARFT-delivered license, while new ones have to become public sector operators." [94]

[90] Belli, L. and De Filippi, P. (Eds.), *Op. cit.*
[91] Noya, J. (dir.) and others, La imagen de España en China, Real Instituto Elcano de Estudios Internacionales y Estratégicos, January 2007, p. 83.
[92] China Internet Network Information Center, *Statistical Report on Internet Development in China*, January 2013, pp. 6, 17 et seq., available at http://www1.cnnic.cn/IDR/ReportDownloads/201302/P020130312536825920279.pdf (last visited on 25th April 2014). However, some have criticised the abovementioned data for being inaccurate. See for instance, Bell, I., *The Open Debate on Chinese Internet Proliferation*, 22 July 2009, http://www.ianbell.com/2009/07/22/the-open-debate-on-chinese-Internet-proliferation/ (last visited on 25th April 2014)
[93] Bambauer, D.E., *Consider the Censor,* Wake Forest Journal of Law & Policy, Forthcoming; Brooklyn Law School, Legal Studies Paper Nº 218, p.4, available at http://ssrn.com/abstract=1757890 (last visited, 30th January 2015).
[94] Media Consulting Group, *The Potential for Cultural Exchanges between the European Union and Third Countries: The Case of China*, Study, European Parliament, DG for Internal policies, Policy Department B: structural and cohesion policies, April 2009, p. 38, available at http://www.europarl.europa.eu/RegData/etudes/etudes/join/2009/419097/IPOL-CULT_ET%282009%29419097_EN.pdf (last visited on 29th January 2015).

On the other hand, net neutrality is not respected in China. Internet traffic is not treated equally in a non-discriminatory way and restrictions are put in place by the government, mainly for political reasons.[95] But how does the Internet control in China work?

2. Forms of Internet control in China

Internet control in China can be presented in different ways. According to Arsène[96] one can classify the Chinese control exercised on the Internet into three levels: through the Chinese Great Wall, online intermediaries and self-censorship.

The Chinese Great Firewall

First, connectivity outside China can only be done through official networks. Filtering mechanisms prevent access to certain websites. These mechanisms have constituted the so-called "Chinese Great Firewall". Used figuratively in the phrase "Great Firewall of China" [97], [it] denotes the extensive Chinese online censorship system".[98]

Broadly speaking, this type of measures constitutes a form of 'censorship', which, according to the American Civil Liberties Union (ACLU) is the "suppression of words, images, or ideas that are 'offensive'", that "can be carried out by the government as well as private pressure groups." [99]

Technically speaking, the Chinese Great Firewall[100] refers to "software or hardware that controls access to computers for the purpose of network security." [101] China controls the

[95] See for instance, Chinese Computer Information Network and Internet Security, Protection and Management Regulations, 30th December 1997, Section Five, available at http://fas.org/irp/world/china/netreg.htm (last visited on 21st June 2015).
[96] Arsène, S., *The impact of China on global Internet governance in an era of privatized control*, Chinese Internet Research Conference, May 2012, Los Angeles, United States, pp. 2-4, available at https://hal.inria.fr/file/index/docid/704196/filename/circ_14mai.pdf (last visited on 18th June 2015).
[97] Cf. http://www.greatfirewallofchina.org/ (last visited on 31st March 2014)
[98] Hogge, B., A Guide to the Internet for Human Rights Defenders, Barefoot Publishing Limited, 2014, p. 82
[99] ACLU, *What is Censorship?*, 30th August 2006, available at https://www.aclu.org/free-speech/what-censorship (last visited on 18th June 2014)
[100] China devotes particular attention to the US. In fact, it is not difficult to make comparisons between the failed international agreement led by the US, 'ACTA', with China's practices. Cf. Masnick, M., *The Similarity Between ACTA And Chinese Internet Censorship*, 20th January 2010, available at https://www.techdirt.com/articles/20100120/0216537828.shtml (last visited on 14th June 2014); By way of example, the father of the Great Firewall blames the US for not being as honest and transparent as

Internet by keyword filtering; Domain Name System Inspection (DNS Inspection); blocking Internet Protocol (IP) addresses and hijacking domain names; restricting foreign and politically-sensitive sites; user-identification restraints, such as imposing the obligation to submit a Photo ID to the government to create a website[102]; or by the obligation placed over cybercafés to request IDs from its customers[103], among others.

Just to mention some examples, keyword filtering is normally used to prevent unwanted e-mails or to filter posts in social media. Domain Name System injection is carried out by a device (a DNS injector), which is strategically located "inside the network to capture DNS requests. Every time the injector sees a DNS request that matches a blocked domain, it sends a fake DNS reply containing invalid information".[104] The DNS can have vulnerabilities, which can "divert Internet traffic away from legitimate servers and towards fake ones." In other words, a DNS cache can be poisoned if the cache information leads to an incorrect entry.[105] IP blocking constitutes another form of censorship that we need to be aware of,[106] which means that IP addresses (regardless of how many resources are sharing each blocked address) are rendered inaccessible.

Yet, it has been reported that the majority of the Chinese population does not seem to complain about the Great Firewall.[107] Maybe this could be explained by the fact that the Chinese government has admitted having learnt propaganda strategies from US

China is with its Internet control policies. Cf. Masnick, M., *Father Of The Great Firewall Defends Chinese Internet Censorship By Noting The US Does The Same Thing*, available at https://www.techdirt.com/articles/20110218/01583213162/father-great-firewall-defends-chinese-Internet-censorship-noting-us-does-same-thing.shtml (last visited on 14th June 2014). That is why in the Press we can find analogical references to the Chinese Great Firewall, such as the 'Great Firewal of America', used by MacKinnon in the New York Times. Cf. MacKinnon, R., *Stop the Great Firewall of America*, 15th November 2011, available at http://www.nytimes.com/2011/11/16/opinion/firewall-law-could-infringe-on-free-speech.html?_r=0 (last visited on 16th June 2014).

[101] Hogge, B., *Op. cit.*

[102] BBC News, *China tightens Internet controls,* 23rd February 2010, available at http://news.bbc.co.uk/2/hi/asia-pacific/8530378.stm (last visited on 15th June 2014).

[103] Abrams, S., *China's Internet Cafes Respond to ID Check Rules*, available at http://www.chinahearsay.com/china-Internet-cafes-respond-id-check-rules/ (last visited on 15th June 2014).

[104] Bonaventure, O., *DNS injection can pollute the entire Internet*, 30th August 2012, available at http://perso.uclouvain.be/olivier.bonaventure/blog/html/2012/08/30/dns_injection_can_pollute_the_entire_internet.html (last visited on 14th June 2014).

[105] See, for instance, http://www.howtogeek.com/161808/htg-explains-what-is-dns-cache-poisoning/ (last visited on 18th June 2014).

[106] Connaught Summer Institute, *Internet Censorship Lab*, 26th July 2013, available at http://www.cs.stonybrook.edu/~phillipa/icl_slides.pdf (last visited on 14th June 2014).

[107] Masnick, M., *Are People In China Happy With The Great Firewall?,* 16th May 2008, https://www.techdirt.com/articles/20080515/0258451120.shtml (last visited on 16th June 2014).

politicians and public relations industry from the US.[108] This, combined with the training Chinese censors and netizens receive, contribute to a distortion of reality, i.e. the existence of violations of human rights online.

In order to show how the Chinese Great Firewall works, to monitor blocked URLs and to show the level of internet censorship in the country, a group of activists set up 'GreatFire.org'.[109] However, this project has been subject to pressure and suffers cyberattacks.[110]

In addition to projects like GreatFire.org, there are tools or technologies which allow circumventing the Chinese Great Firewall, e.g. by using a virtual private network (VPN). As the New York Times reported, "[s]ome foreign companies use Gmail as their corporate email service, for example". Therefore, when being in China, companies "have to ensure that employees have V.P.N., or virtual private network, software to get into Gmail", for example.[111] According to Google's own transparency report on traffic, some of its products and services are subject to disruptions in China, such as Gmail, Google Search, Google sites or Youtube (which is blocked since 2009).[112] 'FireTweet' is another example of alternatives to censorship. 'Firetweet' is an application which allows you to use Twitter in China, as it is widely blocked.[113]

On the other hand, experience in other countries demonstrates that China is getting ready to conquer the Internet.. Several studies confirm this assertion. According to Elcano Global presence 2014 index, China has the fourth biggest presence in the world

[108] Masnick, M., *China Learned The Tricks of Propaganda From The Best: US Politicians & PR Industry,* 5th June 2014, https://www.techdirt.com/articles/20140604/12125327461/china-learned-tricks-propaganda-best-us-politicians-pr-industry.shtml (last visited on 15th June 2014)
[109] https://en.greatfire.org/ (last visited on 15th June 2014).
[110] Gilbert, D., *Chinese anti-censorship group GreatFire.org hit by aggressive DDoS attack*, 23 March 2015, available at http://www.ibtimes.co.uk/chinese-anti-censorship-group-greatfire-org-hit-by-aggressive-ddos-attack-1493105 (last visited on 12th April 2015).
[111] New York Times, *Gmail is blocked in China after months of disruption*,30th December 2014, available at http://www.nytimes.com/2014/12/30/technology/gmail-is-blocked-in-china-after-months-of-disruption.html?hp&action=click&pgtype=Homepage&module=second-column-region&region=top-news&WT.nav=top-news&_r=1 (last visited on 5th January 2015).
[112] Google, *Transparency Report on Traffic*, 2015, available at http://www.google.com/transparencyreport/traffic/disruptions/#region=CN&expand=Y2015 (last visited on 5th January 2015).
[113] Fullerton, J., *This App Lets China's Netizens Use Twitter Where It's Censored*, 9th June 2015, available at http://motherboard.vice.com/read/this-app-lets-chinas-netizens-use-twitter-where-its-censored (last visited on 9th June 2015).

in terms of economic performance, military forces and soft power.[114] The Media Consulting Group conducted a study for the European Parliament, in which it demonstrated that the Internet in China is the "largest in the world and is growing at a fast pace"[115], together with the mobile sector. The OECD confirmed this assertion.[116]

At various occasions, the Great Firewall provoked some websites to become inaccessible in Chile and in the US due to an alleged "mistake" from China's side.[117] Indeed, such could happen thanks to DNS cache poisoning, and, particularly IP address blocking.[118] "Errors" also tend to happen elsewhere. For instance, in the 2014's anniversary of the massacre of Tiananmen Square, LinkedIn censored posts about the massacre in Hong Kong "by mistake", the company said.[119]

China's sway is likely to start from the East of Asia. In fact, a recent report of the Center for Strategic and International Studies demonstrates that China is going to become the most influential power in East Asia in the next decade.[120] Pursuant to a survey conducted from 24th March to 22nd April 2014, more than half of the 402 non-governmental experts consulted from 11 countries (Australia, Burma/Myanmar, China, India, Indonesia, Japan, Singapore, South Korea, Taiwan, Thailand and the United States of America) estimated that China's influence will be relevant. By 2030, "China alone will probably have the largest economy" on top of the US.[121]

---

[114] Olivié, I., Gracia, M. and García-Calvo, C., *Informe Elcano de Presencia global*, Real Instituto Elcano, 23rd April 2014, available at http://www.globalpresence.realinstitutoelcano.org/es/data/Presencia_Global_2014.pdf (last visited on 10th January 2015).
[115] Media Consulting Group, *Op. cit.*, pp. 35-39.
[116] OECD, *China, Information Technologies and the Internet*, OECD Information Technology Outlook 2006, OECD Publishing, pp. 139-182, available at 10.1787/it_outlook-2006-6-enpp (last visited on 29th January 2015).
[117] Masnick, M., *DNS Screwup Accidentally Extends Great Firewall Of China To Chile And The US?,* 26th March 2010, available at https://www.techdirt.com/articles/20100326/2241128746.shtml (last visited on 15th June 2014).
[118] http://www.howtogeek.com/161808/htg-explains-what-is-dns-cache-poisoning/ (last visited on 18th June 2014).
[119] Guilford, G., *LinkedIn is censoring posts about Tiananmen Square*, 4th June 2014, available at http://qz.com/216691/linkedin-is-censoring-posts-about-tiananmen-square-even-outside-mainland-china/ (last visited on 15th June 2014).
[120] Green, M.J. and Szechenyi, N., *Power and Order in Asia. A Survey of Regional Expectations, Center for Strategic and International Studies*, 5th June 2014, available at http://csis.org/files/publication/140605_Green_PowerandOrder_WEB.pdf (last visited on 9th June 2014).
[121] NIC, *Global Trends 2030: Alternative worlds*, US National Intelligence Council, p. III, available at http://globaltrends2030.files.wordpress.com/2012/11/global-trends-2030-november2012.pdf (last visited on 11th June 2014)

Intermediaries in China

The second level of Internet control is exercised by intermediaries. 'Intermediaries' is a broad term "referring to any company providing services on, or to connect to, the Internet."[122] More precisely, the OECD defines them as companies which "give access to, host, transmit and index content, products and services, originated by third parties on the internet or provide internet-based services to third parties." These include Internet access and service providers (ISPs), Data protessing and web hosting providers (including domain name registars), Internet search engines and portals, E-commerce intermediaries or participative networking platforms"[123]

In China, intermediaries providing a service, such as blog hosting, are liable for the content published by Internet users. The law obliges them whether to hire employees to conduct content surveillance or to implement automatic filtering systems, failing which forums of discussions can be closed.[124] Article 15 of the 'Measures on the Administration of Internet Information Services'

> "stipulate what have come to be known as the 'nine forbidden content categories' for Chinese online services. These categories include speech that 'harms the dignity or interests of the State', or 'disseminates rumours, disturbs social order or disrupts social stability', or 'Sabotages State religious policy or propagates heretical teachings or feudal superstitions'."[125]

In this sense, the Chinese's latest campaign buildss on an initiative called "Cleaning the Web 2014", which is a form of information management, i.e. restricting access to information on the grounds of being rumours, pornography, among others.[126]

Failure to comply with or adapt to Chinese Internet policy obligations may entail criminal liability, which can go up to prison,[127] financial liability and, in case of an

[122] McNamee, J., *The Slide From "Self-Regulation" to corporate censorship*, EDRi booklet, 25th September 2011, available at https://edri.org/wp-content/uploads/2010/01/selfregualation_paper_20110925_web.pdf (last visited on 29th June 2015).
[123] OECD, *The Economic and Social Role of internet Intermediaries*, April 2010, p. 9, available at http://www.oecd.org/internet/ieconomy/44949023.pdf (last visited on 16th June 2015).
[124] Arsène, S., *Protester sur le web chinois (1994-2011), Le Temps des médias*, 2012, p. 102, available at https://hal.archives-ouvertes.fr/hal-00773738/document (last visited on 28th January 2015).
[125] UNESCO, *Fostering Freedom Online. The Role of Internet Intermediaries*, 19th January 2015, p. 32, available at http://unesdoc.unesco.org/images/0023/002311/231162e.pdf (last visited on 28th January 2015).
[126] ECFR, *China's Expanding Cyberspace*, June 2014, p. 11, available at http://www.ecfr.eu/page/-/ChinaAnalysisEng_June2014.pdf (last visited on 17th June 2014).

undertaking, the loss of its business license.[128] In fact, Article 20 of the Measures for Managing Internet Information Services allows China to have a strict liability regime. As a UNESCO study points out, [129]

> "[the] Chinese government imposes liability for unlawful content on all intermediaries. If they fail to sufficiently monitor user activity, take down content or report violations, they may face fines, criminal liability, and revocation of business or media licenses."

By imposing intermediary liability, search engines like Google would be obliged not to show websites in its search results (i.e. to de-index them) if the websites in question *inter alia* contain keywords which may endanger the public interest. Failure to comply with such obligation would entail liability, being sanctioned pursuant to the law.

According to the abovementioned UNESCO study, Article 13 of the Chinese Measures on the Administration of Internet Information Services stipulates that

> "all 'information service providers' [ISPs] are required to 'ensure that the information that they provide is lawful'. A revised 'deliberation draft' of the Measures was jointly released by the State Information Office and Ministry of Industry and Information Technology in 2012, proposing a number of updated provisions specifying the obligations of ISPs.
> The draft which is expected to become law and which **has therefore already begun to influence company behaviour**, stipulates that once an internet information service discovers that the information published falls into the nine forbidden content categories', it shall 'immediately stop the publication and transmission thereof, save the relevant records and make a report thereon to the relevant authority and the public security department' (Articles 18 and 19). Article 25 stipulates the creation of a complaints system enabling any member of the public to report illegal content that they see on information service providers to the public security bureau and other relevant government departments."[130] (emphasis added).

In addition, China adopted a new national security law[131] and is expected to adopt a new cyber security law[132], which will further increase pressure on ISPs companies to keep policing online content.

---

[127] E.g. Hu Jia ("incentivising subversion of state power", April 2008); Huang Qi ("illegal possession of state secrets", July 2008); Liu Jin ("using heretical organisation to undermine implementation of the law", November 2008). Cf. Reporters Without Borders, available at https://en.rsf.org/ (last visited on 28th January 2015).
[128] Anonymous, China and the Internet, Harvard International review, Summer 2009, Vol. 31 Issue 2.
[129] UNESCO, Fostering Freedom…, *Op. cit*., p. 40.
[130] *Ibid.,* p. 45.
[131] The National People's Congress of the People's Republic of China, *China adopts national security law*, Press release, Beijing, 1st July 2015, available at http://www.npc.gov.cn/englishnpc/news/Legislation/2015-07/01/content_1940329.htm (last visited on 5th August 2015).
[132] The National People's Congress of the People's Republic of China, *China Seeks public views on new cyber security law*, Press release, Beijing, 8th July 2015, available at

Self-censorship

The third level of Internet control in China is self-censorship.

We live in an era in which self-censorship is a reality. Both the industry and individuals self-regulate and self-censor either because the law imposes this, or because they "voluntarily" want to do so or because there is a lack of trust in the digital environment. This does not solely happen in China, but around the world as well.

Since 1996, Internet users in China had to register with the local police to be able to have Internet subscription. According to Arsène, that does not seem applicable nowadays. Nevertheless, since 2009, Chinese Internet users have to identify themselves with the corresponding Internet service provider to open an account so as to benefit from the service in question. This is called the 'real names system', which is also imposed in hotels, cybercafés or which is required for opening a blog or a microblog.[133]

Fortunately for anonymity and the right to privacy, the enforcement of these restrictive measures does not seem to be perfect, since much of the information provided is not thoughtfully verified. However, the "Regulation on the Management of Internet User Accounts", which was enacted by China's State Internet Information Office on 4th February 2015 and entered into force on 1st March 2015,[134] reinforces the 'real names system'. It strengthens the enforcement of this system by vesting the Cyberspace Administration of China with supervision powers.[135] Privatised enforcement is also encouraged. When the information provided by the user or its/her/his account name is false, harmful, unlawful or fraudulent, "Internet information providers" are required to punish the Internet user, punishment which can go up to the elimination of the account

http://www.npc.gov.cn/englishnpc/news/2015-07/10/content_1941413.htm (last visited on 5th August 2015).

[133] Arsène, S., *The impact of China…, Op. cit.,* pp. 2-4.

[134] Unofficial translation made by China Copyright and Media, China's State Internet Information Office: Regulation on the Management of Internet User Accounts, 4th February 2015, available at https://chinacopyrightandmedia.wordpress.com/2015/02/04/internet-user-account-name-management-regulations/ ; Chinese version available at http://www.cac.gov.cn/2015-02/04/c_1114246561.htm (last visited on 22nd June 2015).

[135] *Ibid*, Article 3.

and to reporting the situation to the "Internet information content controlling department".[136]

Furthermore, Internet users are being told by government-related sources that they are subject to surveillance and are encouraged self-censor.[137] Anonymity is no longer guaranteed on the Chinese Internet.[138] In the words of Arsène, many Chinese online users "lack self-confidence when it comes to writing their opinions online." Website "moderators have the power to delete messages and they often do so"[139] – to the detriment of human rights and fundamental freedoms.

Self-censorship in China can be presented in other forms, such as 'prepublication censorship', which consists of blocking key words and putting in place police cartoons so as to warn users about online content infringements; 'post-publication censorship', which refers to the elimination of blog entries or search engine results; use of sophisticated hacking and cyber-espionage activities; or recourse to manipulation by means of the so-called '50 Cent Party', purportedly composed of 250,000 people, who disseminate favourable ideas about the government and monitor Internet policy compliance.[140]

In this sense, fundamental rights and freedoms are difficult to defend in China, even when users try to use circumvention tools. China is keeping up with new technologies to the point it has been able to interrupt encrypted communications that use a virtual private network (VPN) connection.[141]

What is more, the Chinese government is using education as a means to teach individuals about how to "properly" use the Internet. The already-mentioned Chinese White Paper regarding the Internet further specifies that "[t]he state proactively

[136] *Ibid*, Articles 7 and 8.
[137] Arsène, S., *Protester…, Op.cit,* p. 103.
[138] Unless Internet users circumvent Internet control mechanisms, which are increasingly harder to use effectively due to the power of the technology used by the Chinese government.
[139] Arsène, S., *Online discussions in China. China Perspectives, French Center for Research on Contemporary China*, 2008, p.11, available at https://hal.archives-ouvertes.fr/hal-00773584/document (last visited on 14th December 2014).
[140] Anonymous, *China and the Internet*, *Op. cit*., pp. 71 et seq.
[141] The Guardian, *China tightens 'Great Firewall' Internet control with new technology*, 14th December 2012, available at http://www.theguardian.com/technology/2012/dec/14/china-tightens-great-firewall-Internet-control (last visited on 14th June 2014).

promotes industry self-regulation and public supervision."[142] In fact, the government has launched a code of conduct for the Internet and "Seven Self-Censorship Guidelines", which have already "punished" a considerable number of netizens.[143] China has issued more precise guidelines for celebrities to help them conduct self-censorship[144] and also conducts general trainings on censorship.[145] Additionally, the Internet Society of China (ISC), a national organisation created in 2001 with the view to "serv[e] the development of that industry, netizens, and the decisions of the government", has already issued various sets of self-regulatory recommendations and pledges.[146] Put simply, Chinese people are being taught how to limit expressions of what they think, how to act and react. The Chinese population do not generally have a notion of the level of Internet control in their country.

In sum, China does not count with a global Internet, but with a shaped (restricted) "Chinanet".[147] In line with China's position, Herold considers that the Internet is transforming into an inter-connected national intranets in which China is setting the 'rules of the game'. For Herold, China did not have to control the Internet because everything was state-owned when the Internet was created. On the contrary, the Chinese government had to "explicitly or implicitly allow everything that happens [offline] in [the] Chinese cyberspace."[148] In his words,

> "[t]he Internet used to be a wild, unregulated, border-less place for pioneers and individualists. This began to change as Civilisation arrived to protect the weak and facilitate the exploitation of economic resources. Robber-barons of the Internet arose (e.g. Google) who are still wielding a lot of power (2011), but their era will soon end, as civilisation expands and the state gets ready to challenge their powers. The wilderness is settled and made habitable for all through infrastructure improvements and the elimination of dangers. 'Settled areas' are created (Facebook, Twitter, 'Apps') and 'the

[142] Information Office of the State Council of the People's Republic of China, *Op. Cit.*
[143] Global Voices Advocacy, *China: Over 100,000 Weibo Users Punished for Violating 'Censorship Guidelines'*, 13th November 2013, available at http://advocacy.globalvoicesonline.org/2013/11/13/china-over-100000-weibo-users-punished-for-violating-censorship-guidelines/ (last visited on 14th June 2014)
[144] Global Voices, *China Gives Internet Celebrities a Guide for Self-Censorship*, 13th August 2013, available at http://globalvoicesonline.org/2013/08/13/china-creates-guideline-for-Internet-celebrities-self-censorship/ (last visited on 14th June 2014)..
[145] Sloan, A., *China ramps up army of "opinion monitors"*, 25th March 2014, available at http://www.indexoncensorship.org/2014/03/china-opinion-monitors/ (last visited on 15th June 2014).
[146] Information Office of the State Council of the People's Republic of China, *Op. Cit.*
[147] ECFR, *China 3.0*, November 2012, p. 101, available at http://www.ecfr.eu/page/-/ECFR66_CHINA_30_final.pdf (last visited on 17th June 2014).
[148] Herold, D.H., *An Inter-nation-al Internet: China's contribution to global Internet governance?*, 5th September 2011, pp. 4 and 5, available at http://ssrn.com/abstract=1922725 (last visited on 24th April 2014).

> law' has arrived to watch over the now settled territories ready to join 'the Union' (offline world)."[149]

Herold predicts countries will follow the Chinese model. If so, instead of having access to a "global" Internet, we will live in an "inter-nation-al Internet".[150] "From the United States to the European Union to the Middle East to Africa and Asia, governments have articulated different rationalisations and implemented varying strategies for controlling the Internet".[151] The Internet is part of what Shapiro called the "Control Revolution".[152] In the next section, we demonstrate EU countries also employ forms of Internet control which are sometimes similar to those of China.

3. Forms of Internet control in EU countries

In this section, we analyse the level of Internet control measures in the European Union following the same classification as in the previous section. [153] Broadly speaking, Internet control measures can also be implemented through censorship mechanisms, intermediaries' interventions and self-censorship. However, there are other types of Internet control measures which would not fit this classification, but that still compromise citizens' conduct towards the Internet. An example of Internet control measures implemented within the EU[154] is the Spanish Citizens' Security law. On 29th November 2013, the Spanish government proposed a draft law on the Protection of Citizens' Security, which was intended to substitute an existing law from 1992. On 11th July 2014, the Spanish Council of Ministers adopted the Citizens' Security Bill,

[149] *Ibid*., p. 9.
[150] *Ibid.,* p. 14.
[151] Tai, Z., The Internet in China: Cyberspace and Civil Society, Ed. Routledge, New York, 2006, p. 85
[152] Shapiro, A., The Control Revolution: How the Internet is Putting Individuals in Charge and Changing the World. Public Affairs, New York, 1999.
[153] Arsène, S., *The impact of China…, Op. Cit.*
[154] We could mention more examples, such as the comparison between the Google China case and UK Digital Economy Bill. Cf. MacKinnon, R., *Google and Internet Control in China. Congressional-Executive Commission on China*, 24th March 2010, available at http://rconversation.blogs.com/MacKinnonCECC_Mar24.pdf; Marks, K., *The BPI's China-like clauses in the Digital Economy Bill*, 23rd March 2010, available at http://epeus.blogspot.be/2010/03/bpis-china-like-clauses-in-digital.html; or Masnick, M., *China Gleefully Uses UK Desire For Censorship To Validate Its Own Censorship,* 12th April 2011, available at https://www.techdirt.com/articles/20110812/10553415491/china-gleefully-uses-uk-desire-censorship-to-validate-its-own-censorship.shtml (last visited on 15th June 2014).

"hearing" the opinions of several public authorities and civil society.[155] After being reviewed by the two Parliamentary chambers, the law was adopted on 30th March 2015[156] and entered into force on 1st July 2015.[157]

The Spanish Citizens' Security Law poses several threats to fundamental rights and freedoms,[158] having similarities with some Chinese provisions,[159] to the point that after its adoption, this law was sent to the Spanish Constitutional Court by almost all political parties of the opposition[160] and has been subject to international and national outcry.[161]

As mentioned elsewhere,[162] Article 25 of the Spanish Citizens' Security Law may infringe EU data protection and privacy legislation[163] because it would *inter alia* require cybercafés and related establishments to scan and keep record of their clients' IDs in order for the clients to have access to their services. Failure to do so leads to pecuniary sanctions ranging from 100 to 30,000 Euros.[164]

---

[155] Spanish Minister of Interior, *Aprobado el Proyecto de Ley Orgánica de Protección de la Seguridad Ciudadana*, Press conference, available at http://www.interior.gob.es/web/interior/prensa/noticias/-/asset_publisher/GHU8Ap6ztgsg/content/id/2230243 (last visited on 17th July 2014).

[156] Ley Orgánica 4/2015, de 30 de marzo, de protección de la seguridad ciudadana, Spain, available at http://www.boe.es/diario_boe/txt.php?id=BOE-A-2015-3442 (last visited on 28th June 2015).

[157] ElMundo, *Las 44 conductas que se multan en la nueva 'ley mordaza'*, 1st July 2015, available at http://www.elmundo.es/espana/2015/07/01/559418d5268e3eb16d8b4582.html (last visited on 2nd July 2015).

[158] See, for instance, Rights International Spain and others, *Análisis de la Ley Orgánica 4/2015, de 30 de marzo, de Protección de la Seguridad Ciudadana a los efectos de la posible vulneración de los artículos 1, 9.2, 10.1, 14, 15, 20, 21, 24 y 25 de la Constitución Española*, available at http://rightsinternationalspain.org/uploads/publicacion/3d3d492cacc2a6705ccec427f61dd51b86c0f94b.pdf (last visited on 8th June 2015).

[159] Fernández Pérez, M., Spanish Citizens' Security Bill: Many restrictions, few freedoms, 28th January 2015, available at https://edri.org/spanish-citizens-security-bill-many-restrictions-few-freedoms/ (last visited on 28th January 2015).

[160] Namely, PSOE, la Izquierda Plural, UPyD, Coalición Canaria and Compromís-Equo. The appeal was sent on 21st May 2015. See, for instance, RTVE, *La oposición recurre ante el Tribunal Constitucional la ley de seguridad ciudadana*, 21st May 2015, available at http://www.rtve.es/noticias/20150521/oposicion-recurre-ante-tribunal-constitucional-ley-seguridad-ciudadana/1148155.shtml (last visited on 28th June 2015).

[161] Fernández Pérez, M., *Spanish Citizens…Op. cit.*

[162] Fernández Pérez, M., *Spain: Why you should care about the Citizens' Security Bill*, 30th July 2014, available at https://edri.org/spain-citizens-security-bill/ (last visited on 3rd November 2014)

[163] Article 36(26) of the Spanish law 4/2015, on the Protection of Citizens' Security is another example of a restriction to data protection. See, for instance, Rights International Spain and others, *Op. cit.*, p. 33.

[164] Fernández Pérez, M. and Massé, E., *Spanish Citizens' Security Bill: Many restrictions, few freedoms*, 28th January 2015, available at https://edri.org/spanish-citizens-security-bill-many-restrictions-few-freedoms/ (last visited on 12th April 2015).

Spain is not the only country with such a measure. France also contains an obligation for cybercafés to retain personal data which could identify their users.[165] As noted by scholar Abrams, this measure was implemented in China a few years ago[166] with significant business losses and other countries also unsuccessfully tried to implement such measure. In Chile, its Parliament tried to impose registration of cybercafé users, but the Constitutional Court of Chile declared the proposal unconstitutional.[167]

Following this introduction and EU-related example, in this section we take the same approach as in the previous section (related to China) to easily demonstrate that EU countries also conduct Internet control measures which are detrimental to Internet users' rights and freedoms online.

Censorship

The EU and its Member States are not exempt from being compared to China in terms of censorship.[168] Following Cox, "authoritarian governments who are aggressively blocking and censoring the Internet" are not the greatest danger to "the most powerful engine for […] the free exchange of ideas ever invented", but democratic governments.[169] Masnick expresses the same degree of concern:

> "The slippery slope to censorship starts with the insistence that the mechanism for censorship only has "the best intentions." But the reality is that once you have the infrastructure for censorship, it's only a matter of time until that censorship expands. It's just too powerful for those in control." [170]

[165] Article L34-1 of the "Code des postes et des communications électroniques français", available at http://www.legifrance.gouv.fr/affichCode.do?cidTexte=LEGITEXT000006070987 (last visited on 12th April 2015).
[166] Abrams, S., *Op. cit.*
[167] Constitutional Court of Chile, Court ruling of 12th July 2011, available at http://www.tribunalconstitucional.cl/wp/ver.php?id=2011 (last visited on 28th January 2015).
[168] McNamee, J., *EU and China adopt harmonised approach to censorship*, 18th May 2011, available at http://edri.org/edrigramnumber9-10eu-china-censorship-Internet/; and Masnick, M., *EU Parliament Wants China To Join ACTA, Even As It May Reject It?,* 25th May 2012, available at https://www.techdirt.com/articles/20120524/03204119058/eu-parliament-wants-china-to-join-acta-even-as-it-may-reject-it.shtml (last visited on 16th June 2014).
[169] Cox, C., *Establishing Global Internet Freedom: Tear Down this Firewall*, In Thierer, A. and Crews, C.W. (Eds.), Who rules the net? Internet governance and jurisdiction, Washington D.C., The Cato Institute, 2003, pp. 3-11; Cf. Herold, D.H., *Op. cit,* p. 11.
[170] Masnick, M., *Chinese Lessons For SOPA/PIPA: The Great Firewall Of China Was Once A Way To Stop Infringement Too*, 23rd January 2012, available at https://www.techdirt.com/articles/20120119/17271917481/chinese-lessons-sopapipa-great-firewall-china-was-once-way-to-stop-infringement-too.shtml (last visited on 15th June 2014)

China often argues the Great Firewall is not about censorship, but about protecting public interests.[171] Yet, the same argument is used by Occidental regulators when imposing restrictions to human rights online. By following the same reasoning as in Western countries, China transforms public policy objectives as a justification to censor, intimidate, restrict access or, more generally, to impose online control mechanisms. For instance, China has used this excuse comparing itself to Germany, Turkey, the US or with companies like Facebook[172] or Google.[173]

The main difference, however, is that in China Internet users have been educated not to have access to the global Internet and do not usually see violations of their human rights or fundamental freedoms as a threat. Conversely, Internet users living in democratic countries have a different background. The Internet is open by nature. However, when Internet access is limited, citizens' rights and freedoms become less enforceable.[174] As the Council of Europe recommended, "[t]he freedom, dignity and privacy of Internet users must be a central concern and priority for democracies, especially governments which rely upon and encourage the use of new technologies".[175] The current challenge for democratic governments and companies is to regain citizens' trust. The risk of regaining Internet users' trust is that governments and companies use it as the basis for having more control over the Internet.

This control in democratic countries like EU Member states can be presented in the form of censorship, which adopts different forms. In order to demonstrate censorship exists in EU countries, we provide three examples: media restrictions, content moderation and blocking.

---

[171] Masnick, M., *China: Great Firewall isn't censorship, it's safeguarding the public*, 21st October 2011, available at https://www.techdirt.com/articles/20111020/03291216428/china-great-firewall-isnt-censorship-its-safeguarding-public.shtml (last visited on 15th June 2014).

[172] Eg. Global Times, *Web regulation in public's best interest*, 4th June 2013, http://www.globaltimes.cn/content/786493.shtml (last visited on 14th June 2014);

[173] Masnick, M., *That's Rich: China Accuses Google Of Censorship*, 28th October 2009, available at https://www.techdirt.com/articles/20091027/1754316700.shtml (last visited on 15th June 2014).

[174] Kulesza, J., *Protecting Human Rights Online -- An Obligation of Due Diligence*, Jean Monnet Working Paper 24/14, 2014, p. 11, available at http://www.jeanmonnetprogram.org/papers/14/documents/JMWP24Kulesza.pdf (last visited on 5th January 2015). Although the author refers to freedom of expression, we are of the opinion that the same applies to all fundamental rights and freedoms.

[175] Council of Europe, *Internet Governance Strategy 2012-2015*, available at https://wcd.coe.int/ViewDoc.jsp?id=1919461 (last visited on 2nd January 2015).

First, there have been cases registered for restricting freedom of the media online. For instance, the civil society organisations Index on Censorship and *Osservatorio Balcani e Caucaso* are working on a project to map freedom of the media violations in Europe. [176] At the time of writing, the project has identified over 550 violations in the European Union.[177] Freedom of expression is being threatened with intermediary liability especially on social media. For instance, after a Spanish politician passed away in May 2014, several entries in social media were taken down, leading censorship in social media that was not always proportionate or necessary as some Internet users have faced penalties up to imprisonment.[178]

Second, as Arsène argues, while the role of Chinese 'website moderators' "is often described as crude censorship by Western Internet observers"[, they] tend to forget that this function is also crucial on the Western Web platforms".[179]

Third, blocking represents another form of censorship which is not always proportionate, necessary or efficient. Whereas in repressive states blocking access to the Internet does not surprise many people, western countries are rapidly and dangerously increasing blocking content which is deemed harmful or inappropriate. This system presents at least five flaws. First, blocking can wrongly prevent access to lawful content or permit access to unlawful content. Second, blocking systems like in the UK are possible thanks to lists of targeted websites which are "opaque at best [and] secret at worst".[180] Third, the concept of legality is not the same in all countries, which makes it difficult to assess the nature of the content and the appropriate action to take. Fourth, effective remedies often represent a burden are widely unknown or do not even exist. Fifth, blocking is not very difficult to circumvent from a technical point of view. In this sense, those Internet users willing to have access to unlawful material are decreasingly

[176] Similarly, the civil society organisation Reporters without borders issues a worldwide report assessing the freedom enjoyed by journalists, the media and netizens on a yearly basis. The study takes into account the actions of the governments in order to protect freedom of expression and, in particular, the freedom of the press in its broad sense. Cf. Tout l'Europe, *La liberté de la presse en Europe*, 15th January 2015, available at http://www.touteleurope.eu/actualite/la-liberte-de-la-presse-en-europe.html (last visited on 16th January 2015).
[177] For more information, see http://mediafreedom.ushahidi.com/ (last visited on 15th January 2015).
[178] Fernández Pérez, M., *Spain: social media to be censored? "Not everything is appropriate",* 21st May 2014, http://edri.org/spain-social-media-to-be-censored-not-everything-is-appropriate/ (last visited on 19th June 2014).
[179] Arsène, S., *Online discussions in China…, Op. cit.,*p. 11.
[180] Commissioner for Human Rights, *The rule of law*…, *Op. cit*., pp. 66 and 67.

using websites and rather use "peer-to-peer networks, chat rooms, encrypted web spaces, image hosting sites or hacked sites".[181] Blocking becomes more dangerous when intermediaries are encouraged to take action.[182]

The role of intermediaries

The rule of law is greater challenged when EU countries ask intermediaries to take "voluntary" measures in order to attain public interests, such as protecting children online, countering terrorism or fighting against hate speech.[183] In pursuing these objectives, however, companies become gatekeepers in policing content online. As already stated elsewhere, there is a consistent problem in the European Union when restrictions are imposed in a "voluntary" way by corporations in the absence of a legal obligation. In fact, "there is a broad lack of clarity as regards the extent to which the negative obligations of states are invoked when they encourage private companies to impose restrictions. Similarly, there is a lack of clarity as to the state's positive obligations to react in cases where there are restrictions imposed with or without state involvement."[184] These practices are commonly known as "self-regulation".

The European Economic and Social Committee (EESC), which is one of the EU institutions,[185] defined this practice. According to the EESC, "self-regulation has its origins in behavioural psychology. When applied to the economic sphere, it broadly denotes the adoption by economic operators of certain rules of conduct among themselves or in relation to third parties in the market and in society, adherence to which is agreed among themselves, *without any external coercive mechanisms*" (emphasis added). Nonetheless, as the EESC itself recognises, self-regulatory practices are not always "spontaneous". They can be imposed as long as they serve as a complement to hard law. However, this safeguard can be bypassed if there is a legal basis for these "voluntary" measures. The big loophole in the EU legal framework, as the EESC notes, is that "neither the EU treaties nor Member States' constitutions

[181] Commissioner for Human Rights, *The rule of law…*, *Op. cit*., pp. 66-68.
[182] *Ibid*, p. 70.
[183] *Ibid*, p. 66.
[184] McNamee, J. and Fernández Pérez, M. (Eds.), Human Rights Violations Online, drafted by European Digital Rights for the Council of Europe, DGI(2014)31, 4th December 2014, p. 25, available at https://edri.org/files/EDRI_CoE.pdf (last visited on 30th January 2015).
[185] To know more about the EU institutions, bodies and agencies, see http://europa.eu/about-eu/institutions-bodies/ (last visited on 2nd July 2015).

provide any such enabling basis". The European Commission confirmed that in their 2002 Action plan: "unlike co-regulation, self-regulation does not involve a legislative act".[186]

"[W]hat is still lacking[187] is a political-legislative discussion to clearly define the legal framework that should govern the operation of these instruments at EU level. This should specify their legal nature, lay down conditions for their validity, define their areas of application, clarify links with hard law, and set down their limits in a consistent, coherent and harmonised framework", the EESC Opinion added.[188] Without a clear, legally binding and enforceable legal framework, there will always be a risk of arbitrary behaviour or over-implementation of "voluntary" agreements by intermediaries, sometimes bypassing the rule of law. For instance, some companies like Microsoft state in their terms of service or "code of conduct that they reserve "the right, at its sole discretion, *and without any obligation to do so*, to review and remove user-created services and content at will and without notice, and delete content and accounts" (emphasis added). [189]

Filtering and blocking content online are two examples of these encouraged "self-regulatory" measures taken by intermediaries, encouraged by EU governments.

In fact, some EU countries have or are proposing measures (whether legislative or not) for ISPs to be in charge of taking down or blocking websites whose content could purportedly incite terrorism, for example. However, such classification does not count with judicial review, i.e. no judge verifies the content incites terrorism or not which, indirectly, risks creating a degree of impunity for offenders, who no longer need to reckon with having a real investigation of their activities.

---

[186] European Commission, *Action Plan "Simplifying and improving the regulatory environment",* Communication from the Commission, COM(2002) 278 final – Not published in the Official Journal, 5th June 2002, p.11, available at http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=URISERV:l10108&from=EN (last visited on 2nd July 2015). Cf. EESC, *Opinion on Self-regulation and co-regulation in the Community legislative framework*, INT/754, 22nd April 2015, available at http://www.eesc.europa.eu/?i=portal.en.int-opinions.32859 (last visited on 28th June 2015).

[187] The EESC Opinion dates of 28th April 2015. At the time of writing, such political and/or legal discussion has not taken place yet.

[188] EESC, *Op. cit.*

[189] Microsoft, Code of conduct, updated in April 2009, available at http://windows.microsoft.com/en-us/windows-live/code-of-conduct (last visited on 2nd July 2015).

In the view of the Commissioner for Human Rights for the Council of Europe, these practices represent "a problematic proposition which, along with other filtering measures, could be used to silence undesired voices."[190] These are the practices one finds in France or the UK, for instance.

On 4th March 2015, the French government adopted a decree aimed at further countering terrorism online and its incitement as well as fighting against child pornography.[191] This decree was enacted to complement the French law enacted in 2014 to strengthen the fight against terrorism.[192] Both pieces of legislation reformed the law on trust in the digital economy (the so-called "LCEN").[193] According to Article 6-1 of the LCEN, the French Ministry of Interior has the power to order to blocking certain websites that may *inter alia* incite terrorism. For that, the Ministry needs to warn the hosting company before asking internet access providers to block the allegedly problematic websites.

Between the middle and the end of March 2015, the Ministry of Interior ordered Internet access providers to block five websites in France.[194] In this case, the companies hosting those websites were not notified of the blocking order, contrary to the provisions of the law. This was allegedly due to the fact that the hosting companies were located abroad.[195] According to the LCEN, the Minister of Interior has to ask the

---

[190] Commissioner for Human Rights, *Positions on counter-terrorism and human rights protection*, CommDH/PositionPaper(2015)1, Council of Europe, p. 7, available at https://wcd.coe.int/com.instranet.InstraServlet?command=com.instranet.CmdBlobGet&InstranetImage=2757196&SecMode=1&DocId=2274090&Usage=2 (last visited on 16th June 2015).

[191] Décret [français] n° 2015-253 du 4 mars 2015 relatif au déréférencement des sites provoquant à des actes de terrorisme ou en faisant l'apologie et des sites diffusant des images et représentations de mineurs à caractère pornographique, available at http://legifrance.gouv.fr/affichTexte.do;jsessionid=?cidTexte=JORFTEXT000030313562&dateTexte=&oldAction=dernierJO&categorieLien=id (last visited on 2nd July 2015).

[192] Loi [française] n° 2014-1353 du 13 novembre 2014 renforçant les dispositions relatives à la lutte contre le terrorisme, available at http://www.legifrance.gouv.fr/affichTexte.do;jsessionid=734BDF263C832C9D3D0CD91191F5F5C8.tpdila24v_2?cidTexte=JORFTEXT000029754374&dateTexte=29990101 (last visited on 4th July 2015).

[193] Loi [française] n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique, available at http://legifrance.gouv.fr/affichTexte.do;jsessionid=2509631E5AE8978FD31614987761D29B.tpdila23v_1?cidTexte=JORFTEXT000000801164&dateTexte=20150629 (last visited on 2nd July 2015).

[194] BBC News, French government orders website block, 26th March 2015, available at http://www.bbc.com/news/technology-31904542 (last visited on 26th April 2015).

[195] L'OBS, *Cinq sites "faisant l'apologie du terrorisme" bloqués pour la première fois en France*, 16th March 2015, available at http://tempsreel.nouvelobs.com/societe/20150316.AFP1833/cinq-sites-internet-bloques-pour-apologie-du-terrorisme-une-premiere-en-france.html (last visited on 26th April 2015). This was confirmed by the owner of one of the affected websites, www.islamic-news.info. Cf. Greenwald, G., *What's scarier: terrorism, or governments blocking websites in its name?*, The Intercept, 17th March

website owner to "voluntarily" remove the offensive content, failing which the Minister of Interior asks the Internet service providers to block the websites in question. [196]

As Greenwald puts it, "[i]sn't the exercise of this website-blocking power what has long been cited as reasons we should regard the Bad Countries — such as China and Iran — as tyrannies (which also usually cite "counterterrorism" to justify their censorship efforts)?"[197]

The system described in France is a law-based system, but there are EU systems which do not have a law-based, predictable (even to the limited extent that the French system is) legal framework, as they are "voluntary" or "self-regulatory" agreements between the government and Internet Service Providers to take action to protect children (e.g. child pornography) or to fight against hate speech, for example. This is the case of the UK, for instance.

The British civil society organisation Open Rights Group launched a project to document the impact of "parental control" filters in the UK and help people and companies which have experienced censorship in the UK due to the filtering system to unblock websites. Thanks to this project, "Web users can use a free checking tool on www.blocked.org.uk where they can instantly check to see if a website has been blocked by filters." [198] At the time of writing, Open Rights Group has tested over 2,280,290 sites already. Among the 100,000 top sites rated by the Consultancy firm Alexa,[199] over 20,000 are blocked by strict filters and over 11,000 are blocked by default filters by at least one ISP.[200] Why would some of the top-visited websites be blocked by ISPs?

The practices described above go against the recommendations given by the former UN Special Rapporteur on Freedom of Expression, Frank La Rue, i.e.:

2015, available at https://firstlook.org/theintercept/2015/03/17/whats-scarier-terrorism-governments-unilaterally-blocking-websites-name/ (last visited on 26th April 2015).

[196] Greenwald, G., *Op. cit.*

[197] *Ibid.*

[198] Open Rights Group, *ORG's Blocked project finds almost 1 in 5 sites are blocked by filters*, available at https://www.openrightsgroup.org/press/releases/orgs-blocked-project-finds-almost-1-in-5-sites-are-blocked-by-filters (last visited on 14th May 2015).

[199] Cf. http://www.alexa.com (last visited on 4th July 2015).

[200] Cf. https://www.blocked.org.uk/ (last visited on 4th July 2015).

> "Censorship measures should never be delegated to a private entity, and [...] no one should be held liable for content on the internet of which they are not the author. Indeed, no State should use or force intermediaries to undertake censorship on its behalf."[201]

What is more, the Special Rapporteur further recommended intermediaries to "only implement restrictions to these rights *after* judicial intervention" (emphasis added) [202] In other words, both France and the UK have not followed his recommendations. In this sense, the 2015 Latvian Presidency of the Council of the European Union officially recognised that self-regulatory measures to block or discriminate on content may raise legal concerns vis-à-vis the Charter of Fundamental Rights and the e-Privacy Directive, "including respect of confidentiality of communications."[203]

Self-censorship

Following the classification outlined when examining forms of self-censorship in China and, for the purposes of this paper, we classify self-censorship practices into two types, namely 'pre-publication censorship' and 'post-publication censorship'.

Both means of self-censorship are not only conducted by Internet users, but also by companies. While pre-publication censorship is caused by restrictions to the right to privacy, post-publication censorship is mainly due to freedom of expression restrictions online. In order to exemplify the threats to the right to privacy and freedom of expression that self-censorship cause in the European Union, we mention the so-called 'Delfi case', which was brought before the European Court of Human Rights (ECtHR) by the company Delfi against Estonia[204].

---

[201] UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Report, 16th May 2011, A/HRC/17/27, para. 43, available at http://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf (last visited on 4th July 2015).
[202] *Ibid,* para. 47.
[203] Latvian Presidency of the Council of the European Union, *Proposal for a Regulation of the European Parliament and of the Council laying down measures concerning the European single market for electronic communications and to achieve a Connected Continent, and amending Directives 2002/20/EC, 2002/21/EC and 2002/22/EC and Regulations (EC) No 1211/2009 and (EU) No 531/2012 - Examination of the Presidency compromise text on net neutrality*, 1 3555/13 TELECOM 232 COMPET 646 MI 753 CONSOM 161 CODEC 2000, 20th January 2015, p.3, available at http://data.consilium.europa.eu/doc/document/ST-5439-2015-INIT/en/pdf (last visited on 9th July 2015).
[204] ECtHR, Grand Chamber, *Delfi AS v. Estonia*, Application No. 64569/09, 16th June 2015, available at http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-155105#{%22itemid%22:[%22001-155105%22]} (last visited on 14th July 2015).

Delfi is a major Internet news portal in Estonia which allows posting comments below the articles it publishes. In order to prevent unacceptable behaviour by Internet users, Delfi had put three mechanisms in place. First, an automatic filtering system which automatically deletes comments with obscene words (i.e. a pre-publication self-censorship tool). Second, a notice-and-take-down system by means of which any Internet user could notify Delfi of hate speech, insulting or mocking comments and Delfi would "expeditiously" remove the comments in question (i.e. a post-publication self-censorship tool). Third, a removal mechanism under which any victim of defamation could notify Delfi of a defamatory comment so Delfi could delete it immediately (i.e. a pre-publication self-censorship tool).[205]

Internet users were able to comment on the articles without being registered.[206] In other words, Delfi decided not to impose a real name policy for commenters, therefore preserving users' anonymity and privacy online.

In January 2006, one of the articles Delfi published was widely commented. Some of the comments, however, were of a defamatory nature. The defamation victim notified Delfi six weeks after the publication of the article of the comments and asked for damages. Delfi removed the comments on the same day, but refused to pay the damages claimed. [207]

The victim of the defamatory comments sued Delfi before the Estonian courts. After going through different instances, the Estonian Supreme Court ruled against Delfi. [208] Despite Article 15 of the E-commerce Directive, Estonia's Supreme Court ruled Delfi had to monitor and censor unlawful content prior to its publication.[209] As stated elsewhere, "[t]he Supreme Court of Estonia found that safe harbours set in the e-Commerce Directive did not apply to Delfi, as the hoster of the comments. It based its argumentation on para. 42 of the Preamble of the e-Commerce Directive that indicates that the safe harbour exceptions [only] cover cases where the activity of the

[205] *Ibid*, paras. 11-13.
[206] *Ibid*, para. 12.
[207] *Ibid*, paras. 16-19.
[208] Supreme Court of Estonia, *Vjatšeslav Leedo v. AS Delfi*, 3-2-1-43-09, 10th June 2009, para. 13.
[209] McNamee, J. and Fernández Pérez, M. (Eds.), *Human Rights Violations Online…, Op. cit.,* p.9.

intermediary is limited to the technical process of operating and giving access to a communication network."[210]

In December 2009, after exhausting the national remedies available, Delfi's lawyers challenged this case before the ECtHR for violation of Delfi's right to freedom of expression, which is embedded in Article 10 of the European Convention of Human Rights. On 10th October 2013, the ECtHR found[211] the restrictions to Delfi's freedom of expression were proportionate. Additionally, the ECtHR found that Delfi's pre-publication and post-publication self-censorship tools were not sufficient to ensure third-party personality rights were respected, "taking into consideration the economic interest deriving from the number of comments and the technical capacity of the ISP."[212] The case was referred to the Grand Chamber of the ECtHR, which confirmed the finding. The Court received numerous *amici curiae* from civil society organisations and industry organisations, in favour of Delfi. Nevertheless, the Court remained firm and concluded no breach of Delfi's freedom of expression had taken place.

In line with the E-commerce Directive,[213] Delfi can be considered as an Internet hosting service provider in the EU. [214] According to its Article 14, hosting service providers can be held liable for third party content if they become aware of illegal activities or information hosted by them and do not act "expeditiously" to remove or prevent access to the controversial activity or information. Article 15 of the e-commerce Directive prohibits Member States from imposing a general monitoring obligation on ISPs. With these safe harbour provisions, hosting providers only have two legal incentives, i.e. avoiding liability and eventual damages. However, no counterbalancing incentive to respect human rights online is placed on hosting providers (or other ISPs). The risk of over-censoring or -monitoring is only counteracted by a customer service policy or good public relations for defending freedom of expression.[215] This risk is evidenced in

[210] *Ibid.*
[211] ECtHR, *Delfi AS v. Estonia*, Application no. 64569/09, 10th October 2013, available at http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-126635#{%22itemid%22:[%22001-126635%22]} (last visited on 14th July 2015).
[212] McNamee, J. and Fernández Pérez, M. (Eds.), *Human Rights Violations Online…, Op. cit.,* p.10.
[213] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market, available at http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32000L0031&from=EN (last visited on 7th July 2015).
[214] A type of Internet Service Provider (ISP).
[215] McNamee, J. and Fernández Pérez, M. (Eds.), *Human Rights Violations Online…, Op. cit.,* p.8.

the Delfi case. Not alone did Delfi lose its case before several instances, but cases like this one pushed the Estonian company to adopt stricter measures. Following this case, other ISPs may adopt a "real name policy" – to the detriment of all Internet users' privacy and freedom of expression's rights – and more extensive pre- or post-publication self-censorship tools to avoid facing liability and paying for damages.

Yet, in the so-called 'Telekabel case', which was brought before the Court of Justice of the European Union (CJEU), [216] the CJEU "relied on an assumption that the pressures (an injunction) for the internet intermediary to restrict access [due to alleged intellectual property rights infringements] were counterbalanced by unspecified other obligations to uphold users' fundamental rights."[217] This is evidenced in para. 63 of the CJEU ruling, which states that:

> "even though the measures taken when implementing an injunction such as that at issue in the main proceedings are not capable of leading, in some circumstances, to a complete cessation of the infringements of the intellectual property right, they cannot however be considered to be incompatible with the requirement that a fair balance be found, in accordance with Article 52(1), in fine, of the Charter, between all applicable fundamental rights, provided that (i) they do not unnecessarily deprive internet users of the possibility of lawfully accessing the information available and (ii) that they have the effect of preventing unauthorised access to protected subject-matter or, at least, of making it difficult to achieve and of seriously discouraging internet users who are using the services of the addressee of that injunction from accessing the subject-matter that has been made available to them in breach of the intellectual property right."

As stated elsewhere, "[t]hat suggests that, if the *Telekabel* assumption is incorrect [as the ECtHR seems to argue in Delfi's case], the legal framework needs to be updated."[218]

[216] Court of Justice of the European Union, *UPC Telekabel Wien GmbH v Constantin Film Verleih GmbH, Wega Filmproduktionsgesellschaft mbH*, C-314/12, 27th March 2014, available at http://curia.europa.eu/juris/document/document.jsf;jsessionid=9ea7d2dc30d5a910a3a8a4864c3fb194fea0fadffd3a.e34KaxiLc3qMb40Rch0SaxuQbhf0?text=&docid=149924&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=51610 (last visited on 14th July 2015).
[217] McNamee, J. and Fernández Pérez, M. (Eds.), *Human Rights Violations Online…, Op. cit.,* p.11.
[218] *Ibid.*

III. HUMAN RIGHTS ONLINE

Once seen the different mechanisms of control in both China and the EU, we focus on the framework under which Human rights and fundamental freedoms must be respected in each case.

But what do we mean when we refer to Human Rights?

The Constitutional law expert Peña González considers that the topic of human rights relates to the positioning of men vis-à-vis power in its various manifestations, i.e. the power held by the State or the government against the liberty of those who obey the ones in power.[219] Peña González differentiates between Human rights and Fundamental rights. Whereas Human rights are the subjective rights of individuals, Fundamental rights are subjective rights which are materialised into laws, including a Constitution, and are sometimes internationalised. They are universal, inalienable (i.e. their ownership is untransferable), imprescriptible (i.e. even if they are not exercised, they cannot be waived).[220] More precisely, the Vienna Declaration and its Programme of Action state that "human rights are 'universal, indivisible and interdependent and interrelated'".[221] Peña's approach allows us to understand that even if in countries like China Human rights are enshrined in the law, they have a different stand as, for example, EU countries. For the purposes of this paper, we only refer to "human rights".

In previous chapters, we identified examples of violations of human rights and fundamental freedoms online. In this section, we further explore whether the human rights online situation in China is very different from the situation in the EU or its Member States. Although the baseline scenario and policy making is different in substance, we argue there are several fissures in the EU legal framework which lead us to argue that human rights and freedoms are being eroded inside the European Union. Besides the democratic principles and strong legal framework and enforcement, improvements in policy- and decision-making are needed.

[219] Peña González, J., Derecho y Constitución, Ed. Dykinson S.L., Madrid, 2004, pp. 494, 495.
[220] *Ibid*, p.497.
[221] OHCHR, *Vienna Declaration and Programme of Action*, 25th June 1993, para. 5, available at http://www.ohchr.org/EN/ProfessionalInterest/Pages/Vienna.aspx (last visited on 29th January 2015).

We first explore the different perspectives in both China and the European Union as regards the enjoyment of and restrictions to human rights and fundamental freedoms online. Secondly, we further analyse this situation by focusing on two examples: the right to privacy and freedom of expression. Finally, we make an assessment on the right to an effective remedy. The Internet has become an unprecedented tool for the promotion of freedom of expression and freedom of association or freedom of collective action. However, it also generates risks to privacy, the protection of personal data or security. Yet, there is a common global legal standard according to which restrictions to human rights and freedoms must be imposed by law. If human rights and freedoms are limited, citizens must thus have the right to an effective remedy. Is this complied with in the same way in China and in the EU?

1. Human Rights online in China as compared to the EU

According to the UN Human Rights Council Resolution on promotion, protection and enjoyment of human rights on the Internet of July 2012,[222] human rights offline must also apply online. We are of the view, however, that human rights offline cannot be directly translated online due to the particularity of the Internet, due to its complexity and technology development.

The Internet has been and is a human rights enabler. Nonetheless, the Internet has become a tool which can be used to threaten its users in an unprecedented manner; in a way that the offline world did not know before.[223] Professor Jakubowicz identifies four ways in which Information and Communications Technologies (ICTs)[224] have an impact on human rights:

[222] UN Human Rights Council, The promotion, protection and enjoyment of human rights on the Internet, UN Doc. A/HRC/20/L.13, 5th July 2012.
[223] Kulesza, J., *Protecting Human Rights Online…, Op. cit.,* p. 2.
[224] "Information and Communication Technologies (ICTs) are a collection of technologies and applications that enable the electronic storage, retrieval, processing and transfer of data to a wide variety of users: individuals, households, enterprises from most of the industries and public sector organisations. The Information Society describes a society where ICT, especially the Internet and mobile phones, affect many and different levels of society and the economy." Understood in its broader sense, it plays a key development role in both social and economic terms. Cf. CSIL and PPMI, *Internet, digital agenda and economic development of European regions*, Directorate-General for Internal Policies, Policy Department B: Structural and Cohesion Policies, Study, Vol. I., for the European Parliament's Committee on Regional Development, PE 513.970, September 2013, pp. 13-15, available online at http://www.europarl.europa.eu/studies (last visited on 29th January 2015).

First, ICTs have a multiplier effect on human rights, by adding a new dimension to their exercise, protection and violation. Second, ICTs have a quality impact on human rights, by providing new possibilities to protect and exercise human rights and to present criminal actions. Third, ICTs can influence some human rights to the point of redefining them, by way of "adding cyberspace as a new universe for their exercise". The right of free elections is a clear example of this. Fourth, ICTs have the ability to enhance human rights in a way never experienced before, but at the same time ICTs may create divisions based on those who do not benefit from ICTs yet. Such is the case of freedom of expression or freedom of assembly and association.[225]

In **China**, there are new forms of censorship that are being further developed, as we discussed in Chapter two. In the future, it is likely it will be more difficult to measure different forms of censorship and this is not only happening in China, but around the world. China's practices of restricting freedom of expression and privacy rights, for instance, are being replicated in other countries, but China learns from other countries as well.

Many rights of the Chinese citizens are set forth in the law, such as the public's right to access information, the right to be heard or the right to privacy. However, those rights and freedoms must be exercised *in accordance with the Chinese law*.[226] The problem is that the Chinese understanding of the rule of law differs from the international or the European concept of the rule of law.[227]

The concept of the 'rule of law' in China was coined by the reform policy launched by Deng Xiaoping in 1979. It differs from the western concept of 'rule of law' because in China the 'rule of law' goes along with the Socialist system with Chinese characteristics. On 23rd October 2014, at the 4th Plenary Session of the 18th Central Committee of the Chinese Communist Party, the latter undertook a Decision to "accelerate the construction of a Socialist rule of law country", moving forward the

[225] Jakubowicz, K., *Media revolution in Europe: ahead of the curve*, Council of Europe Publishing, August 2011, pp. 120-123.
[226] Information Office of the State Council of the People's Republic of China, *Op. cit.*
[227] In the EU, this principle is enshrined in Article 52 of the Charter of Fundamental Rights of the European Union.

country in accordance with the law.[228] "The Party comes first"[229], that is, the government has wide discretion to enact legislation to stop practices which it does not deem appropriate in accordance with its communist system, principles and ideology enshrined in the law and thus has the ability to sanction them.[230]

The Chinese notion of the rule of law does not correspond with the requirements set forth under international law. In fact, the legality principle would not be enough in order for China to fulfil its obligations under the 'rule of law' principle. As the UN Secretary-General established in its 2004 report,[231]

> "the rule of law [is] a principle of governance in which all persons, institutions and entities, public or private, including the State itself, are accountable to laws that are publicly promulgated, equally enforced and independently adjudicated, and which are consistent with international human rights norms and standards. It requires, as well, measures to ensure adherence to the principles of supremacy of law, equality before the law, accountability to the law, fairness in the application of the law, separation of powers, participation in decision-making, legal certainty, avoidance of arbitrariness and procedural and legal transparency."

China does not seem to qualify to respect the rule of law according to such criteria. Matheny shows this contradiction very well:

> "In 2011, the UN Human Rights Council condemned the arbitrary blocking or filtering of information on the Internet in its "Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression." The report singled out China specifically stating, "China, which has in place one of the most sophisticated and extensive systems for controlling information on the Internet, has adopted extensive filtering systems that block access to websites containing key terms such as 'democracy' and 'human rights'. The Special Rapporteur is deeply concerned that

[228] Scholars Drs. Roger Creemers and Jeremy L. Daum translated the decision into English, cf. Central Committee of the Chinese Communist Party, Decision to "accelerate the construction of a Socialist rule of law country", 28th October 2014, available in English at https://chinacopyrightandmedia.wordpress.com/2014/10/28/ccp-central-committee-decision-concerning-some-major-questions-in-comprehensively-moving-governing-the-country-according-to-the-law-forward/ (last visited on 11th January 2015).

[229] Subba, B.B., *18th CPC Central Committee Fourth Plenum: Rule of Law with Chinese Characteristics*, Institute of Chinese Studies, No. 22, Delhi, November 2014, available at http://www.icsin.org/ICS/ICSAnalysispdf/32.pdf (last visited on 11th January 2015).

[230] See Peerenboom's analysis of the Decision of 23rd October 2014 at Peerenboom, R., *Fly High the Banner of Socialist Rule of Law with Chinese Characteristics! What Does the 4th Plenum Decision Mean for Legal Reforms in China?,* 6th November 2014, available at http://ssrn.com/abstract=2519917 (last visited on 11th January 2015).

[231] UN Secretary-General, *Report on the Rule of Law and Transitional Justice in Conflict and Post-Conflict Societies*, S /2004/616, 23rd August 2004, para. 6, available at http://daccess-dds-ny.un.org/doc/UNDOC/GEN/N04/395/29/PDF/N0439529.pdf?OpenElement (last visited on 11th January 2015).

> [Internet censorship has become] increasingly sophisticated, with multi-layered controls that are often hidden from the public." [232]

Ironically, every member of the UN Human Rights Council, including China, signed the 2012 resolution to protect human rights on the Internet. The idea that internet should come unrestricted is obviously popular but, as with many issues the UN tackles, a signature can sometimes mean very little. China's delegate stipulated that "free flow of information on the Internet and safe flow of information on the Internet are mutually dependent," in a sign that the country is not about to tear down the "Great Firewall of China" anytime soon**.**" [233]

Is this China's fault or is it a problem of international law, one may wonder. Mattei and Nader offer an interesting and unpopular perspective, arguing the problem arises from international law. "To judge aspects of the rule of law to be illegal in a fundamental sense requires indigenous legal standards separate from nation state and modern globalized legal structures", they argue. In fact, international human rights is "a problematic notion because it provides a selective justification for intervention in the internal political business of all states that are not culturally aligned with Western or imperial rule of law." "International law thus has an ambiguous relationship with the imperial rule of law. While one would think that its development and centralization might limit the imperial sovereign and thus establish legality, in fact it establishes double standards and political non-accountability",[234] they add. Peerenboom seems to agree:

> "China lacks the soft power to challenge the global dominance of the liberal democratic conception of rule of law. Liberals will continue to push for reforms consistent with the globally dominant conception, and critics at home and abroad will, fairly or unfairly, continue to assess reforms and measure China against the standard of liberal democratic rule of law."[235]

But are these contradictions in the conception of the 'rule of law' reflected in the way in the **European Union**?

---

[232] Matheny, S., *Net Neutrality: The Struggle for Internet Freedom*, 30th September 2013, available at http://globalsolutions.org/blog/2013/09/Net-Neutrality-Struggle-Internet-Freedom#.VYaIjUa1dcM (last visited on 21st June 2015).
[233] *Ibid.*
[234] Mattei, U. and Nader, L., Plunder. When the Rule of Law is Illegal, Blackwell Publishing, United Kingdom, 2008, p. 153.
[235] Peerenboom, R., *Fly High the Banner…, Op. cit.*, p.20.

The immediate answer is 'no, they are not' because of the strong and generally enforceable legal and political framework in the EU. However, there have been cases where restrictions to fundamental rights and freedoms have been violated in a disproportionate way.

Concerning the rule of law, McNamee very well summarises the situation: "[T]he rule of law is affirmed four times in the Treaty on European Union. It is "confirmed" in the preamble of the Treaty and restated in Article 6. The EU also places an obligation on itself to contribute to the objective of consolidating "democracy and the rule of law" in its development policy (Article 21) and common foreign and security policy (Article 22). Furthermore, the European Convention on Fundamental Rights and the Charter of Fundamental Rights place obligations on EU Member States and on the Commission (ratification of the European Convention of Human Rights, the "ECHR", is pending) that restrictions to freedoms must be based on law."[236]

Besides this strong legal framework in favour of the rule of law, cases of censorship are not absent, as we have seen in Chapter two.

In sum, the differences of both systems seem clear. Freedom of expression will not be truly enjoyed unless respect of privacy in communications is ensured.[237]

Even if international law applies to the Chinese people, there is a lack of enforcement – to the detriment of the population of China. Freedom of speech and the right to privacy, as recognised in the Universal Declaration of Human Rights and in the ICCPR are two clear examples of regular violations of human rights online in China. So the question that should be asked is, can the international legal framework be enforced to promote freedom of expression and protect privacy online?

---

[236] McNamee, J., *Privatised online enforcement series: A. Abandonment of the rule of law*, 23rd March 2011, available at https://edri.org/edrigramnumber9-6abandonment-rule-of-law/ (last visited on 21st June 2015).

[237] Cf. paras. 76, 77, 81-99 of the Human Rights Council, Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue, U.N. Doc. A/HRC/23/40. See also Office of the High Commissioner on Human Rights, State communication surveillance undermines freedom of expression, warns UN expert, 4th June 2013, available at: http://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=13400&LangID=E (last visited on 29th January 2015).

2. Restrictions to freedom of expression and privacy

Internet innovation technologies have allowed netizens to enjoy freedom of expression at its fullest. Nevertheless, technology has been and can be used to impair civil rights and liberties, among which freedom of expression and the right to privacy are of particular relevance.

China has a different approach than Europe.

On the one hand, it formally recognises **freedom of speech** in its Article 35 of the Chinese Constitution. Although China would comply with the legality principle, it would not be enough in order for China to respect the 'rule of law', as explained before.

According to the Information Office of the State Council of the People's Republic of China, however,

> "Chinese citizens fully enjoy freedom of speech on the Internet. The Constitution of the People's Republic of China confers on Chinese citizens the right to free speech."[238] "The Internet provides unprecedented convenience and a direct channel for the people to exercise their right to know, to participate, to be heard and to oversee, and is playing an increasingly important role in helping the government get to know the people's wishes, meet their needs and safeguard their interests. The Chinese government is determined to unswervingly safeguard the freedom of speech on the Internet enjoyed by Chinese citizens in accordance with the law." [239]

From 2000 onwards, information society services provided in China increased in a very significant way. The start of the XXI century was marked by the proliferation of electronic commerce services, such as Taobao, which is the Chinese equivalent to Ebay or Amazon.

Social networks also marked the beginning of the first decade of the XIX century. Xiaonei (whose name "Renren"), for instance, was launched in 2005, which is a similar network as Facebook. In 2010, Weibo represented the success of the microblogging phenomenon in China. [240] The expansion of microblogs like Weibo has allowed sharing and receiving information in a way unexperienced before in China. The most known

[238] Information Office of the State Council of the People's Republic of China, *Op. cit.*
[239] Information Office of the State Council of the People's Republic of China, *Op. cit.*
[240] Arsène, S., Protester sur…*Op. cit.*, p. 101.

microblogs in China (Weibo, Sohu, Netease and Tecent) have removed or suspended users' accounts, imposed real-name registration requirements as of 16th March 2012 or hide content (including keywords) which disregards the law. However, some microbloggers have found ways to circumvent repression from the government, by setting up new accounts, using different keywords, among others.[241]

From an international law perspective, China's Internet control policy would violate freedom of expression[242] as enshrined in Article 19 of the Universal Declaration of Human Rights (UDHR) and Article 19 of the International Covenant on Civil and Political Rights (ICCPR).

The UDHR defines freedom of expression as the "freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers". The ICCPR specifies that restrictions may be imposed provided they are applied pursuant to the law and are deemed necessary "[f]or respect of the rights or reputations of others" or "for the protection of national security or of public order (*ordre public*), or of public health or morals."

Whereas China is a signatory party of both international instruments, it has not ratified the ICCPR. By signing, China expressed its willingness or intention to be bound by it. Yet, the ICCPR is not binding on China or transposed meaningfully into Chinese law. In this regard, some scholars argue that even if China signed and ratified the ICCPR, it would do so with many reservations, undermining the importance of its ratification.[243] In the same vein, "the United Nations (UN) Special Rapporteur on Freedom of Opinion and Expression, the Organization for Security and Co-operation in Europe (OSCE) Representative on Freedom of the Media, the Organization of American States (OAS)

[241] Yong, H., Spreading the news, in Schmidt, N. (Ed.), *Digital Frontiers*, Index on censorship, Volume 21. No. 4, Sage Publications, 2012, pp. 107-111.
[242] For a deeper study, see Human Rights Committee, General comment No. 34, Article 19: Freedoms of opinion and expression,102nd session, July 2011, U.N. Doc. CCPR/C/GC/34, paras. 3, 9, 21-23, 25 and 27.
[243] Free Speech Debate, *Article 19: freedom of expression anchored in international law*, 10th February 2012, available at http://freespeechdebate.com/en/discuss/article-19-freedom-of-expression-anchored-in-international-law/ (last visited on 17th June 2014). Other scholars like Joe McNnamee made the case that the opposite is true – a country that is not taking an instrument seriously is less likely to set reservations. See McNamee, J., *Should Reporting-based Human Rights Treaties Be Considered "Binding International law"?*, University of Kent, Brussels, 1st September 2006, available at http://www.ibrarian.net/navon/paper/Should_Reporting_based_Human_Rights_Treaties_Be_C.pdf?paperid=8325925 (last visited on 3rd August 2015).

Special Rapporteur on Freedom of Expression and the African Commission on Human and Peoples' Rights (ACHPR) Special Rapporteur on Freedom of Expression and Access to Information"[244] worked together to issue a yearly Joint Declaration on the International Mechanisms for Promoting Freedom of Expression, in which recommendations are issued mainly for States, but also for other actors. By analysing its latest declaration,[245] we acknowledge their recommendations are too broad and vague to appreciate a precise impact to promote freedom of expression in China.

On the other hand, the right to **privacy** is proven "to be a prerequisite to the capacity to participate in social discourse. Where privacy is dismantled, both the chance for personal assessment of the political and societal process and the opportunity to develop and maintain a particular style of life fade."[246] Yet, privacy is not fully respected in China.

Even if privacy is formally recognised by the State, the official policy position of **China** is the following:

> "[t]he state protects citizens' online privacy. The protection of online privacy is closely connected with the people's sense of security and confidence in the Internet. The Chinese government proactively promotes the improvement of relevant legislation and Internet corporate service regulations, in order to steadily enhance online privacy protection systems. The Decision of the National People's Congress Standing Committee on Guarding Internet Security stipulates that illegal interception, tampering with or deletion of others' e-mails or other data and infringement upon citizens' freedom and privacy of correspondence that constitutes a crime shall be investigated for criminal liability. According to the self-disciplinary public pledges of the Internet industry, Internet service providers are responsible for protecting users' privacy. The providers shall announce their relevant privacy protection commitment when providing services, provide reporting and reception channels for privacy infringement and take effective measures to protect users' privacy."[247]

In the same vein, the Government claims privacy is also protected at the network level. According to the Chinese computer Information Network and Internet Security, Protection and Management Regulations, "the freedom and privacy of network users is protected by law. No unit or individual may, in violation of these regulations, use the

[244] See http://www.osce.org/fom/118298 (last visited on 17th June 2014).
[245] See http://www.osce.org/fom/118298?download=true (last visited on 17th June 2014).
[246] Simitis,S., Reviewing Privacy in an Information Society, 135 U.PA. L. REV. 707, 734, 1987.
[247] Information Office of the State Council of the People's Republic of China, *Op. cit.*

Internet to violate the freedom and privacy of network users." [248] Yet, this is not fully ensured in practice.

From an international perspective, the right to privacy is set forth in both the UDHR and the ICCPR, respectively in Articles 12 and 17. These instruments define this right as the prohibition of arbitrary or unlawful interferences to individuals' privacy, family, home or correspondence and of unlawful attacks to their honour or reputation.

While the non-binding UDHR contains a general restrictive clause in its Article 29 para. 2, which makes the exercise of all rights and freedoms named in the Declaration subject to limitations determined by law "solely for the purpose of securing due recognition and respect for the rights and freedoms of others and of meeting the just requirements of morality, public order and the general welfare in a democratic society", no such general reference or one relating directly to privacy can be found in the ICCPR. However, individual restrictive clauses can be found for other rights, such as Article 19 para. 2, allowing for legitimate limitation of the freedom of expression." [249]

In the **European Union,** both the freedom of expression and the right to privacy are recognised as fundamental rights respectively in Articles 11 and 7 of the EU Charter of fundamental rights. This complements the rights embedded in national law, starting from the constitutions; the rights recognised under international human rights law and the ECHR. Regarding the latter, Article 6(3) of the Treaty on the European Union (TEU) establishes that "fundamental rights, as guaranteed by the European Convention for the Protection of Human Rights and Fundamental Freedoms and as they result from the constitutional traditions common to the Member States, shall constitute general principles of the Union's law." Yet, sometimes these freedoms and rights are violated, as demonstrated in Chapter two of this study.

In sum, China and EU countries have different approaches towards the freedom of expression and the right to privacy. However, this does not mean that the EU is exempt of committing violations to human rights and freedoms online. Yet, when these happen,

[248] Chinese computer Information Network and Internet Security, *Op. cit.,* Section seven.
[249] Kulesza, J., *Protecting Human Rights Online…*, *Op. cit*., p.18.

how do the Chinese system and the European system respond to human rights restrictions online?

3. The Right to an effective remedy

Concerning the situation of redress in **China**, Internet users do not enjoy of an effective remedy in the Western meaning. In this context, the Chinese judicial system has to be understood within the whole Chinese's political, social and legal system.

Guided by the principle of double instance[250], the Chinese judiciary is divided into four levels: the local people's courts, which are subdivided into basic people's courts; intermediate people's courts and higher people's courts[251]; special people's courts (military, railway and transport and maritime courts) and the Supreme People's Court[252].[253] However, China's judicial system is not solely composed of the people's court system, but also of both the people's procuratorate and the public security systems.[254] Strictly speaking, the judiciary comprises the two first ones.

Notwithstanding the lack of accurate and complete empirical data[255], scholars note that the Chinese judicial system is highly affected by various weaknesses. For the purposes of clarity, we have non-exhaustively regrouped them into ten.

First, there is a problem of substance, since most of the restrictions imposed to human rights and freedoms online would not pass the international tests of necessity and proportionality. For instance, in 2013, the Chinese Supreme Court issued a decision that "limit[ed] to 500 the number of times a post [could] be reposted without the original

[250] See Arts. 10 et seq. of the Organic Law of the People's courts of the People's Republic of China.
[251] Art. 2 (3) of the Organic Law of the People's courts of the People's Republic of China.
[252] While the Supreme People's Court is the highest court; the Higher People's Courts are courts of the provinces, autonomous regions and municipalities; the Intermediate People's Courts are for capitals or prefectures within the provincial level; and the Basic People's Courts are for counties, municipal districts and autonomous counties. Moreover, the Basic People's Courts can establish people's district level tribunals (usually in big towns), whose decisions have the same legal effects. For more information, see http://guides.library.harvard.edu/chineselegalresearch (last visited on 20th January 2014).
[253] Arts. 123 et seq. of the Chinese Constitution; art. 11 of the Judges Law of the People's Republic of China of 2001.
[254] See http://www.olemiss.edu/courses/pol324/chnjudic.htm (last visited on 20th January 2014).
[255] With the consequences attached to it, such as unfounded generalised statements; cf. Clarke, D. C., *Empirical Research Into the Chinese Judicial System*, 15th July 2003, available at http://ssrn.com/abstract=412660 (last visited on 20th January 2014).

author's assuming legal responsibility. Because spreading false rumors is a crime, the decision mean[t] that anyone who writes a popular but subversive post could be held liable and face prison time." [256] A famous case involving imprisonment was the case of writer Yang Tongyan, who was arrested in China 9 years ago due to his writings, involvement in protests, among other charges. He was punished with 12-year imprisonment.[257]

Second, the majority of judges in China lack of technical competences and the judicial system suffers from inefficiency. In 2001, the Judges Law tried to improve the situation by requiring judges to comply with a set of minimum requirements. Their non-fulfilment may lead to dismissal, an obligation to receive training or transfer to non-judicial positions. In addition, inefficiency is also linked to judges' remuneration. Although they have now to pass the same public competition as lawyers and procurators, judges are not well paid, especially those in the lower scales of the judicial hierarchy.[258]

Third, there is a disparity between lower/rural courts and higher/urban ones. Courts set up in poorer areas do not have enough technical, material or human resources.

Fourth, the principle of public hearings is not fully respected. The principle of public hearings is set out in the law,[259] but it is sometimes restricted by the law itself, which imposes limitations in case of state secrecy, individual privacy or crimes committed by minors, among others. Other times, this principle is impaired by material deficiencies related to the budget of some courts. Positively, the law allows parties or the People's "procuracy" to lodge an appeal to annul the decision should this principle be infringed, but the implementation of this mechanism is doubtful. [260]

---

[256] New York Times, *Gregarious and direct China's web doorkeeper*, 2nd December 2014, available at http://www.nytimes.com/2014/12/02/world/asia/gregarious-and-direct-chinas-web-doorkeeper.html (last visited on 5th January 2015).

[257] See his case at http://www.pen.org/defending-writers/test-first-name-test-middle-name-test-last-name/yang-tongyan (last visited on 29th January 2015).

[258] See Art. 9 of the 2001 Judges Law of the People's Republic of China; Cf. Garot, M.-J., *El poder judicial en China: ¿independiente y eficaz?,* InDret, Vol. 2, 2009, May 2009, pp. 12 et seq., available at http://www.indret.com/pdf/629_es.pdf (last visited on 20th January 2014).

[259] Art. 7 of the Organic Law of the People's courts of the People's Republic of China.

[260] Garot, M.-J., *Op. cit*, p.9.

Fifth, the principle of publicity and media coverage is not respected. Notwithstanding the legal reforms encouraged by the entry into the WTO and the efforts carried out by the Supreme People's Court, most of the court rulings are not being published or even drafted, especially at the local level.[261]

Sixth, the rights of defence and the *non bis in idem* principle are impaired. The Chinese system does not offer the same judicial remedies as the Western countries do.[262] For instance, the Supreme People's Court, a higher court or even the procuratorate or the People's "procuracy" are entitled to re-examine a case or ask the lower court to re-decide the case in another way, which puts their impartiality and independence into question. In 2007, the Chinese Civil Procedural law introduced some reforms in this regard, including new possibilities to ask for a new trial or re-examination. Although the fact that the Chinese judicial approach is not the same as the Western approach , this is not automatically a deficiency.Conversely, the reforms put in place do not seem to be sufficient.[263]

Seventh, the most pressing concern is judicial independence, with some analysis suggesting that this is in fundamental contradiction with a single-party communist state.[264] Surprisingly, however, judicial independence in democracies is sometimes narrower than in authoritarian regimes.[265] Contrary to most of the criticisms, the Communist Party of China is not always the main source of interference. Both systemic and non-systemic interferences can be justified in some instances (e.g. the intervention of senior judges could be justified by the lack of experience or competence of lower judges), but what is really important is the impact on the outcome of court cases. The key then becomes to find a balance between accountability and being subject to political, economic or social factors when deciding a case.[266] Following Peerenboom's

[261] *Ibid.*
[262] *Ibid.,* p. 7.
[263] *Ibid.,* p.8.
[264] Although China is officially described as a multi-party country.
Cf. http://www.china.org.cn/english/Political/29034.htm (last visited on 20th January 2014).
[265] See, for instance, Ginsburg*, Law and the Liberal Transformation of the Northeast Asian Legal Complex in Korea and Taiwan,* Fighting for Political Freedom: Comparative Studies of the Legal Complex and Political Change, Oxford: Hart Press, 2007.
[266] García-Bolívar, *Lack of judicial independence and its impact on transnational and international litigation,* Law and Business Review of the Americas 18.1, Winter 2012, p. 30.

thesis, we argue that judicial independence is not a goal in itself, but "a means to a just and efficient judiciary". [267]

According to Peerenboom,[268] 'judicial independence' is a multifaceted concept which consists of decisional, personal, internal, external and collective elements. Decisional independence is achieved when the judicial power is exercised independently pursuant to the law, not being subject to interferences from other parties. However, under the Chinese Constitution, judges experience interferences even within the judiciary.[269] For its part, personal independence is linked to how judges are appointed, promoted and paid and to the impartiality under which cases are assigned to them. The Chinese legislature participates in this process, greatly influencing the most important positions in the judiciary. In China, courts are financed by local governments and the standing committee of local people's congresses may select assessors to participate in a case. In this sense, the latter have the same authority as judges.[270] As a result, this puts pressure on judges to be biased by local protectionism. On the other hand, the internal and external independence of the Chinese judicial system is challenged by two factors. First, judicial rulings may be subject to approval of an adjudicative committee or senior judges. Second, the judiciary is affected by external sources, namely the Party, People's congresses and the "procuracy", local governments and administrations, public opinion or judges' acquaintances.[271] In other words, both the internal and external independence of Chinese judges are not assured. Finally, Professor Peerenboom considers that collective independence is based on the authority of the courts as a whole and on the ability to be free from undue influences. In this sense, much more remains to be done, notwithstanding the recent progress. This is confirmed by results of the Global Competitiveness Report 2014-2015 conducted by the World Economic Forum Report,

[267] Peerenboom, R., *Judicial Independence in China: Common Myths and Unfounded Assumptions*, La Trobe Law School Legal Studies Research Paper No. 2008/11, p. 11, available at http://ssrn.com/abstract=1283179 (last visited on 20th January 2014).
[268] *Ibid*.
[269] Art. 126 of the Chinese Constitution
[270] Art. 38 of the Organic Law of the People's courts of the People's Republic of China.
[271] Fu, Y. and Peerenboom, R., *A New Analytical Framework for Understanding and Promoting Judicial Independence in China*, 1st February 2009, available at http://ssrn.com/abstract=1336069 (last visited on 20th January 2014).

under which China scored 4.0 out of 7. This report includes the assessment of 144 countries and from 1 to 7, 'seven' represents the "best possible outcome".[272]

Eighth, the implementation of decisions is jeopardised because of the lack of cooperation between some agencies; power struggles between the judiciary itself and with the "procuracy" or the ambiguous relations between the Chinese Communist Party and the courts.[273]

Ninth, in a society in which *guantxi* (personal networking) is essential, it is difficult to overcome corruption, which is intrinsically linked to the absence of judicial independence.[274] In fact, China ranked 100 out of 175 countries in the 2014 Corruption Perceptions index. It scored 36 out of 100, being 0 "very clean" and 0 "highly corrupt". Taking the form of bribery and misappropriation, corruption has become so significant that the government is taking direct action to fight it.[275]

In any case, corruption is not the only area in which the government is investing efforts. Indeed, a number of reforms have been carried out to alleviate the aforementioned weaknesses. We focus on two reforms, the 2007 Civil Procedural Law reform and the 2014 Decision of the Communist Party to "accelerate the construction of a Socialist rule of law country".

The abovementioned 2007 Civil Procedural law[276] has set forth procedural economy measures, improvements to litigants' rights, increased transparency[277], enforcement measures or extended implementation deadlines up to two years.[278] Secondly, professionalism of the judicial authorities has been encouraged and existing mechanisms to remove or change judges' positions should they fail to comply with the

[272] Schwab, K. (Ed.) et al., *Global Competitiveness Report 2014-2015*, World Economic Forum, pp. 101, 102 and 155, available at http://www3.weforum.org/docs/WEF_GlobalCompetitivenessReport_2014-15.pdf (last visited on 11th January 2015).
[273] Lubman, S., *Looking for law in China*, Columbia Journal of Asian Law, Spring/Fall, p. 26; Cf. Garot, M.-J., *Op. cit.,* p. 15.
[274] Garot, M.-J.. *Op. cit*., pp. 16 et seq.
[275] Cf. http://www.transparency.org/country#CHN (last visited on 11th January 2015).
[276] Another example is shown in Articles 13, 32 and 33 of the 1997 Criminal Law set forth the criminal liability of judges in these cases. Cf. Garot, M.-J.. *Op. cit*., pp. 16 et seq.
[277] See Ye, A., and Song, Y., *Justice, efficiency and the new Civil Procedure Law,* China Law & Practice, Nov/Dec 2012.
[278] Garot, M.-J., *Op. cit.*.

law have been reinforced.[279] Thirdly, the judiciary has strengthened its authority, as evidenced by the increase of case law or by the fact that most of the cases are not politically sensitive ones, thus reducing the direct inquiries and influence of the Communist Party of China and its organs.[280] Fourthly, the third Supreme People's Court's five-year agenda is enhancing improvements in order to have a more professional, efficient and just system.[281]

On 23rd October 2014, the Chinese Communist Party adopted the abovementioned decision to "accelerate the construction of a Socialist rule of law country", by means of which the Chinese Communist Party tried to improve the judicial system. Professor Peremboom considers that although the Party has tried to conduct a series of reforms which would indeed improve the current judicial system, negative aspects remain.

On the positive side, we can summarise Peremboom's analysis into three main positive aspects. First, the reform tries to increase the efficiency of the system and achieve better justice, e.g. by ensuring court rulings are reasoned and contain a legal analysis and improving their enforcement. Second, the 2014 reform tries to improve the quality and professionalism of judges, by increasing specialisation, requiring an appropriate background for becoming a judge, making meritocratic promotions or tackling corruption. Third, the reform intends to extend access to justice and make more appeals available.

On the negative side, Peeremboom believes human rights' abused by people being put in prison would not suffer any difference in view of the 2014 reform. Secondly, he acknowledges progress on the quality and independence of judges, as those who are best trained usually leave to the private sector and judges are being "educated" the ideology of the Party by the Party itself. Third, disparity between lower/rural courts persists. Fourth, the publicity of court procedures and rulings is improved, but freedom of speech and assembly are further reduced, further controlling the media coverage and

[279] Arts. 14 and 16 of the Chinese Judges Law.
[280] Zhang, X., *A law unto themselves: the Chinese government has acknowledged that corruption in the judiciary is a serious problem,* Hong Kong Lawyer, Vol. Mar, No. 1, Article no. 4, pp. 28-30, 1998, available at http://ssrn.com/abstract=1810187 (last visited on 20th January 2014).
[281] Cfr. Peerenboom, R., *Between Global Norms and Domestic Realities: Judicial Reforms in China*, 8th May 2009, pp. 7 et seq., available at http://ssrn.com/abstract=1401232 (last visited on 20th January 2014).

reducing public petitions.[282] As Professors Liebman and Wu expressed it, "the real question is how often courts fail to decide cases [for] fear of public outcry".[283]

Other scholars believe that the latest reforms imply a shift against the law,[284] as part of a political strategy of the Party to go against the norms. Professor Minzner,[285] for instance, argues that the reforms promote the Communist Party of China's propaganda instead of truly addressing the flaws of China's judicial system.[286] Yet, some scholars like Dr Yuwen Li think that the Chinese's judicial reform is "an unfolding process of modernisation rather than westernisation".[287] In sum, progress has been made to accommodate China's judicial system to international standards of justice, but some core issues remain.

Next to this panorama in China, does the European Union have a remedy system free of criticism?

In the **European Union**, the right to an effective remedy is guaranteed both at the national level and the EU level. EU Member states must abide by the EU Charter of fundamental rights as do the EU institutions. In Article 47 of the Charter, Member states and the EU Institutions must ensure that citizens have the right to an effective remedy and fair trial. That is not only ensured by national courts and the Court of Justice of the European Union, but also applies to other competent parties, such as companies, which are required to provide adequate safeguards when fundamental rights and freedoms have been breached.

[282] Peerenboom, R., *Fly High the Banner…*, *Op. Cit*., pp. 16-19.
[283] Liebman, B. and Wu., T., *China's Network Justice*, Columbia Public Law Research Paper No. 07-143, 9th January 2007, p. 51, available at http://ssrn.com/abstract=956310 (last visited on 26th June 2015).
[284] E.g. Article 22 of the 2007 Civil Procedure Law.
[285] See Minzner, C.F., *China's Turn Against Law*, American Journal of Comparative Law, 2011; Washington University in St. Louis Legal Studies Research Paper No. 11-03-01, available at http://ssrn.com/abstract=1767455 (last visited on 20th January 2014).
[286] "The Internet has become an important channel for people to obtain news. Ever since its introduction to China, the Chinese people have been making full use of the Internet to disseminate news." See Moody, G., *Russia And China Both Want To 'Protect Children'; Both Want To Do It By Increasing Censorship*, 13th July 2012, available at https://www.techdirt.com/articles/20120712/07000519673/russia-china-both-want-to-protect-children-both-want-to-do-it-increasing-censorship.shtml (last visited on 14th June 2014).
[287] Li, Y., The Judicial System and Reform in Post-Mao China: Stumbling Towards Justice, The rule of law in China and Comparative Perspectives, Ed. Ashgate Publishing Limited, England, 2014, p. 245.

Article 47 of the Charter is similar to Article 13 of the ECHR. As the European Commission puts it, "[t]he Charter is consistent with the [ECHR] adopted in the framework of the Council of Europe: when the Charter contains rights that stem from this Convention, their meaning and scope are the same".[288]

In order to approximate arid legal texts to the people, the Council of Europe elaborated a Guide on Human Rights[289] for users as well as an Explanatory Memorandum.[290] As stated elsewhere, [291]

> "the Guide and the Explanatory Memorandum clarify [that] there are different types of remedies. They can adopt the form of an inquiry, an explanation, a reply, a correction, an apology, a reinstatement, reconnection; compensation, among others. Internet users shall have the right to "easily accessible" information about their rights and the remedies. As pointed out in the Explanatory Memorandum, "no single remedy may itself entirely satisfy the requirements of Article 13". Only the "aggregate of remedies provided in law may do so".[292]
>
> Article 13 ECHR solely refers to remedies from national authorities when their rights and freedoms are violated. Nevertheless, as both the Guide and the Explanatory Memorandum explain, every internet user shall have the right to obtain effective redress from ISPs, national and/or European authorities and tribunals."

Europe has a legal framework which allows for an effective remedy, but the key problem the European Union is now facing, most particularly with regard to online restrictions, relates to so-called "self-regulatory" measures, which we briefly referred to in chapter two. These types of measures leave the positive and negative obligations of the twenty-eight Member states of the European Union non enforceable because intermediaries do not have a positive or negative obligation to respect human rights when they cause them online, usually after being encouraged to do so by governments. In other words, EU countries share this problem with China, although to a lesser (but

---

[288] European Commission, *EU Charter of Fundamental Rights*, DG Justice, available at http://ec.europa.eu/justice/fundamental-rights/charter/index_en.htm (last visited on 29th January 2015).
[289] Recommendation CM/Rec(2014)6 of the Committee of Ministers to member States on a Guide to human rights for Internet users, 16th April 2014, available at https://wcd.coe.int/ViewDoc.jsp?id=2184807 (last visited on 15th December 2014).
[290] Recommendation CM/Rec(2014)6 of the Committee of Ministers to member States on a guide to human rights for Internet users – Explanatory Memorandum, 16th April 2014, available at https://wcd.coe.int/ViewDoc.jsp?Ref=CM%282014%2931&Language=lanEnglish&Ver=addfinal&Site=CM&BackColorInternet=C3C3C3&BackColorIntranet=EDB021&BackColorLogged=F5D383 (last visited on 15th December 2014).
[291] McNamee, J. and Fernández Pérez, M., *Op. Cit*., p. 25.
[292] See ECtHR, Silver and others v. UK, no.5947/72; 6205/73; 7052/75; 7061/75; 7107/75; 7113/75; 7136/75 para. 113; Kudla v. Poland, no. 30210/96, para. 157.

growing) extent – due to the political and legal framework that the EU enjoys. We explore the role of online intermediaries in the next chapter.

IV. INTERMEDIARIES VIS-À-VIS HUMAN RIGHTS

As shown throughout this paper, digital rights are increasingly being restricted in many ways by various actors, including governments, ISPs, search engines and, in general, companies working in the Information and Communications Technology (ICT) sector, a set of companies which we gather under the category of "intermediaries". It is important to specifically address them because of the role they play in the digital field. David Kaye, the UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, expressed this concern in his investiture before the UN General Assembly in October 2014:

> "Non-state actors often play a dominant role on the internet today, even in those countries where the government exercises substantial control and regulation. My predecessors and many others have addressed corporate responsibility issues, and I intend to build on their work. For instance, what set of best practices should govern those internet actors with a major footprint in social media, commerce, news, and other subjects? What responsibilities are owed users and customers where privacy interests and expression intersect? How do legal innovations such as the European Court of Justice's so-called right to be forgotten implicate freedom of expression? How can actors implement these policies while avoiding violations of freedom of expression? What are the appropriate reactions of commercial actors when governments demand compliance with rules that are inconsistent with the freedom of expression or other rights that implicate expression?"[293]

This chapter is dedicated to explore those questions. First, we explore the role of foreign intermediaries in China in relation to trade law. Secondly, we explore the framework under which companies are expected to respect human rights online. Thirdly, we conduct a critical assessment on grounds used to restrict human rights and fundamental freedoms online.

[293] Kaye, D., Statement to the 69th session of the UN General Assembly, 23rd October 2014, New York, available at http://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=15220&LangID=E (last visited on 27th June 2015).

1. Foreign companies in China and trade law

China has a tradition of being a protectionist country, but it has evolved throughout the years.[294] This has permitted many foreign corporations –mainly American companies— to access the Chinese internet market due to its potential growth. Some of them have become famous for their restrictive "self-regulatory" practices in China. We explore two examples, Yahoo and Google.

As for Yahoo, a case tarnished its reputation in April 2005, when the company was allegedly obliged to release details of the e-mail account of Shi Thao, a Chinese journalist. Yahoo was asked by the Chinese authorities to release a set of data that included an e-mail the journalist had sent to a Chinese-language site located in the United States. The content of the e-mail was already known by public opinion, but that did not matter. As a result of Yahoo's cooperation, the reporter was condemned to ten years of imprisonment for having leaked "state secrets".[295] Shi Thao has since been released.[296]

Google was also at the centre of attention. When Google decided to set up in China in 2006 under the domain 'google.cn', it accepted to conduct self-censoring practices in order to comply with Chinese law. Otherwise, it would have been held liable for lack of action, as explained in this paper. This decision resulted in international criticism from the western, notably from the US government, human rights organisations and NGOs, asking Google to cease this conduct. Additionally, Google did not succeed in becoming the first engine of the country, as this business was led by the state-owned search engine Baidu.[297] In the beginning, Google justified its practices with a positivist view of the

[294] By imposing restrictions on foreign investment, foreign establishment in China or discrimination measures based on nationality. See, for instance, CCA Advogados, *Legal Guide for Foreign Investors in China*, 20th September 2010, available at http://www.cca-advogados.com/xms/files/Guia_Resumido_ING_02_reduzido.pdf (last visited on 12th January 2015).
[295] Conley, N., *The Chinese Communist Party's New Comrade: Yahoo's Collaboration with the Chinese Government in Jailing a Chinese Journalist and Yahoo's Possible Liability Under the Alien Torts Claim Act*, 15th June 2006, available at http://ssrn.com/abstract=1420373 (last visited on 31st March 2014).
[296] See, for instance, The Guardian, *Shi Tao: China frees journalist jailed over Yahoo emails*, 8th September 2013, available at http://www.theguardian.com/world/2013/sep/08/shi-tao-china-frees-yahoo (last visited on 25th April 2014)
[297] Daxue Consulting, *Overview of the E-commerce Market in China*, 2013, available at http://daxueconsulting.com/overview-of-the-e-commerce-market-in-china/ (last visited on 25th April 2014)

law, by stating it had to comply with Chinese laws, arguing that it was at least providing information to Chinese netizens about its practices.[298] Yet, Google undertook the decision to leave China in 2010, shifting its business to Hong Kong.[299]

Its exit caused many reactions. Some argue Google left because of its non-satisfactory economic performance. Currently, 'Google.com.hk' has become the 14th best positioned site in China.[300] This is not particularly impressive for a company whose 'google.com' site is the most visited around the globe.[301] Others remembered Google's original "Don't Be Evil" motto. The veil of naivety falls once you realise it actually conducts same practices in other countries, or one might be tempted to ask "Will Google Pull Out Of India, Australia And Other Countries Over Internet Censorship [as well]?".[302]

Other foreign companies have been subject to international scrutiny: Apple was criticised for banning Tibet-related apps[303]; Cisco and Sun Microsystems for providing the Chinese Government with the technology to block IP addresses[304]. In return, they have and are facing legal issues. For instance, Cisco was sued twice[305] before US federal courts in 2011 for enabling the Chinese government to "monitor, capture, and kill Chinese citizens for their views and beliefs."[306] In addition, Cisco went through battles concerning its business in China. In 2003, Cisco brought an action against

[298] For an ethical review on Google's activity in China, see Musielak, L.T., *"Google-ing" China: An ethical analysis of Google's censorship activities in the People's Republic*, 2010, available at http://snl.depaul.edu/writing/Googleing%20China.pdf (last visited on 16th June 2014).
[299] See Lee, J-A., Liu, C-Y. and Li, W., *Searching for Internet Freedom in China: A Case Study on Google's China Experience*, 1st April 2013, Cardozo Arts & Entertainment Law Journal, Vol. 31, No. 2, 2013, available at http://ssrn.com/abstract=2243205 (last visited on 18th March 2014).
[300] Alexa, *Top Sites in China*, available at http://www.alexa.com/topsites/countries/CN (last visited on 25th April 2014)
[301] Alexa, *The top 500 sites on the web*, available at http://www.alexa.com/topsites (last visited on 25th April 2014)
[302] Masnick, M., *Will Google Pull Out Of India, Australia And Other Countries Over Internet Censorship?*, 14th January 2010, available at https://www.techdirt.com/articles/20100113/2252047738.shtml (last visited on 15th June 2014).
[303] Tibet Post International, *Tibet-related apps are censored by technology giant Apple*, 5th April 2013, available at http://www.thetibetpost.com/en/news/international/3309-tibet-related-apps-are-censored-by-technology-giant-apple (last visited on 14th June 2014).
[304] Ling, Y., *Op. cit*, p. 17
[305] Cf. District court for the District of Maryland, *Du Daobin, et al. v. Cisco Systems, Inc. et al*., case 8:11-cv-01538-PJM, 24th February 2014, available at https://www.eff.org/files/2014/02/24/4995755-0-12686.pdf (last visited on 13th July 2015); and the so-called "Falung Gong case". See Olukotun, D., *Human Rights Verdict Could Affect Cisco in China*, 24th April 2013, available at http://advocacy.globalvoicesonline.org/2013/04/24/human-rights-verdict-could-affect-cisco-in-china/ (last visited on 15th June 2014).
[306] EFF, *Cisco and Abuses of Human Rights in China: Part 1,* 8th July 2011, available at https://www.eff.org/deeplinks/2011/07/eff-urges-microsoft-and-cisco-to-reconsider-china (last visited on 15th June 2014).

Huawei, a Chinese undertaking which is the "second largest telecommunications equipment company" in the world[307], for allegedly stealing some of its IP assets.[308]

After China's accession to the World Trade Organisation (WTO) in 2010, have these situations changed?

The Information Office of the State Council of the People's Republic of China stated that "China abides by the general obligations and any specific commitment as a WTO member, protects the legitimate rights and interests of foreign enterprises in China, and provides proper services to those enterprises in their legal business operations concerning the Internet."[309]

Since the accession to the WTO, China has opened its frontiers in a greater way. For instance, in 2013, the government set up a new free trade zone in Shanghai, which was followed by the establishment of other twelve free trade zones in others areas of the Chinese Territory.[310] In order to attract foreign investors, China even removed the ban on sites like Facebook, Twitter and the New York Times within the Shanghai Free-Trade Zone.[311] Even though expansion of such policy should be extended beyond Free-Trade Zones, this limited opening is good news.

Nonetheless, as noted by some scholars, the different forms of censorship and Internet control practices in general endanger the compliance with the obligations that China engaged to comply with when becoming a member of the WTO. Measures like

[307] Intelligence and Security Committee, *Foreign involvement in the Critical National Infrastructure. The implications for national security,* June 2013, p. 5, available at https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/205680/ISC-Report-Foreign-Investment-in-the-Critical-National-Infrastructure.pdf (last visited on 14th June 2014).
[308] ComputerWire, *Cisco sues Huawei over IP 'theft'*, 24th January 2003, http://www.theregister.co.uk/2003/01/24/cisco_sues_huawei_over_ip/ (last visited on 25th April 2014); See also Reuters, *Insight: For Cisco and Huawei, a bruising rivalry reaches stalemate*, 22th November 2013, available at http://www.reuters.com/article/2013/11/22/us-cisco-huawei-insight-idUSBRE9AL0NO20131122 (last visited on 14th June 2014).
[309] Cf. Information Office of the State Council of the People's Republic of China, *Op. cit.*
[310] Chen, G., Tsang, D. and Ren, D., *12 new free-trade zones to follow in Shanghai's footsteps*, South China Morning Post, 23rd January 2014, available at http://www.scmp.com/business/china-business/article/1411417/12-new-free-trade-zones-follow-shanghais-footsteps (last visited on 12th January 2015).
[311] South China Morning Post, *China to lift ban on Facebook – but only within Shanghai free-trade zone*, 24th September 2013, available at http://www.scmp.com/news/china/article/1316598/exclusive-china-lift-ban-facebook-only-within-shanghai-free-trade-zone?page=all (last visited on 14th June 2014).

filtering[312] or blocking sites within its Great Firewall can constitute a protectionist measure,[313] when discriminating against foreign companies, with no valid justification.

On the one hand, China could be potentially infringing article XI:1 (non-tariff barrier) and Article XX of the General Agreement on Tariffs and Trade (GATT), since justifying censorship measures for public morals could hardly be accepted by the Panel or the Appellate Body of the WTO, especially because it would be difficult to comply with the standards of Article XX's chapeau. On the contrary, if the Panel or the Appellate Body accepted China's arguments, it would mean that in practice access to the Chinese market was restricted and forced foreign companies to comply with China's demands.[314]

The European Commission pleaded for this possibility.[315] However, through the analysis of three WTO cases, namely the 2008 EU v China on foreign financial information service providers Regulations, the 2009 US v China regarding audiovisual products and the 2009 IP rights enforcement of copyrights, Broude reached the conclusion that trade law and Human Rights law serve different objectives. Whereas trade law's objective is the liberalisation of trade, Human Rights law's goals are stricter. Therefore, any influence trade law could have in China to promote freedom of expression would be secondary or have a side effect. Following western countries' legal reasoning, China justifies Internet policies on the basis of the protection of the general interest.[316]

On the other hand, some scholars have analysed the means available to the US to bring a 'Google China case' before the WTO Dispute Panel. For instance, Gao examines the probabilities of a successful outcome pursuant to the General Agreement on Trade in

[312] Read UNESCO, *Fostering Freedom Online…Op. cit.*, pp. 100-107.
[313] Erixon, F., Hindley, B. and Lee-Makiyama, H., *Protectionism Online: Internet Censorship and International Trade Law*, available at http://www.ecipe.org/media/publication_pdfs/protectionism-online-Internet-censorship-and-international-trade-law.pdf (last visited on 17th June 2014).
[314] Black, E., *China's Internet Censorship Harms Trade, US Companies*, 6th December 2011, available at http://www.forbes.com/sites/edblack/2011/12/06/chinas-Internet-censorship-harms-trade-us-companies/ (last visited on 17th June 2014).
[315] Masnick, M., *Is the Great Firewall of China a Trade Barrier? And If So, Does China Care?*, 17th May 2010, available at https://www.techdirt.com/articles/20100517/0102209437.shtml (last visited on 15th June 2014)
[316] Broude, Tomer and Hestermeyer, Holger P., *The First Condition of Progress? Freedom of Speech and the Limits of International Trade Law*, 5th May 2013, Virginia Journal of International Law, available at http://ssrn.com/abstract=2260969 (last visited on 13th July 2015).

Services (GATS). As a result of his research, Gao concluded that challenging "the Chinese internet censorship regime" based on trade law grounds would be difficult.

First, Gao argues it would be difficult for the US to prove that the services provided by Google would fall within the Schedule of Specific Commitments of China because they are not exactly "value-added telecom services", but "data base services". Even if they were included in the definition of the former, a claim under Articles XVI (market access) or XVII (national treatment) would be hard, at least for "selective filtering". The reason is that even if domestic companies are not subject to the same obligations as foreign companies, that is because the Great Firewall only applies to servers which are located outside China. Besides such technicalities, national websites are subject to other mechanisms of control. They are not subject to filtering. For instance, when an Internet user wants to create a blog post with the words "Falun Gong"[317], an automatic error message is generated. In such a case, there is no need for a Chinese company to filter the content. Accordingly, the fact that domestic and foreign companies are not subject to the same mechanisms of control does not necessarily mean foreign companies are treated in "less favourable" way. The US would need to bring evidence to the contrary to make a case. However, Gao deems more appropriate and easier for the US to resort to Articles VI (domestic regulation) and II (most favoured nation treatment) of the GATS. According to Article VI.I of the GATS, for instance, the US would have to demonstrate that "all [Chinese] measures of general application affecting trade in services are [not] administrated in a reasonable, objective and impartial manner", which seems easier to prove.

Nevertheless, if the US pleaded for GATS violations and succeeded in finding evidence to prove it, China could invoke the exception provided for in Article XIV a) (public morals or public order). In such a case, China would need to demonstrate the measures applied are necessary and do not represent a means of "arbitrary or unjustifiable discrimination".

[317] "Falun Gong" is a spiritual practice, whose practitioners suffered persecution and prosecution in China. See, for instance, Greenlee, M.J., *A King Who Devours His People: Jiang Zemin and the Falun Gong Crackdown: A Bibliography*, International Journal of Legal Information: Vol. 34: Iss. 3, Article 9, January 2006, available at http://scholarship.law.cornell.edu/cgi/viewcontent.cgi?article=1074&context=ijli (last visited on 27th June 2015).

Finally, even if the US won the case, the enforcement of the decision would not be enough to end with China's practices over the Internet. States are only urged to comply with the law; there's no specific enforcement mechanism.[318] The same could apply with a European company which wanted the EU to challenge the Chinese protectionist system via trade law. At the time of writing, there is no known trade case, but a case could still happen.

The European market is not as protectionist as the Chinese market. Both European and Chinese companies should (at least morally) respect human rights online, but there is evidence to sustain that companies sometimes act in an arbitrary way both in China and in Europe. In the next two sections, we explore the grounds for companies to respect human rights and grounds that allow them to restrict Internet users' fundamental freedoms and Human rights.

2. Grounds for companies to respect Human Rights

Due to the societal need for companies to respect human rights in the online environment, the UN established business standards, such as those enshrined in the UN Global Compact (2000), and further elaborated norms regarding the responsibilities of transnational corporations and other forms of business with regard to Human Rights.[319]

On the other hand, ICT companies have taken the initiative to abide by certain principles and behaviours. In fact, there are corporations which have committed to respect codes of conduct to the extent possible, since they are usually based on a voluntary basis. For instance, Google, Microsoft and Yahoo launched the Global network initiative (GNI) in 2006 with the purported aim to advance in the freedom of expression and respect of privacy, although it is difficult to imagine that the avoidance of regulation was not at least part of their motivation.[320] Although the GNI was initially conceived as an initiative for corporations, scholars, investors and some members of the

[318] Gao, H.S., *Google's China Problem: A Case Study on Trade, Technology and Human Rights Under the GATS*, Asian Journal of WTO & International Health Law and Policy (AJWH), Vol. 6, pp. 347-385, 2011, available at http://ssrn.com/abstract=1976611 (last visited on 31st March 2014).
[319] For more information, see Business & Human Rights Resource Centre, available at http://business-humanrights.org/en/un-secretary-generals-special-representative-on-business-human-rights (last visited on 22nd January 2015).
[320] See https://globalnetworkinitiative.org/faq/index.php (last visited on 17th June 2014).

civil society have committed to abide by it. What is interesting to note is the hegemony of the American nationality of the (few) companies represented.[321] The rather crass contradiction between the demands of the GNI principles that governments do not restrict human rights arbitrarily and the arbitrary rights to restrict fundamental rights that are contained in those same companies terms of service is also difficult to overlook.

As regards China, when businesses decide to enter the Chinese market, they need to decide whether to follow the rules of the game, fight against them or exit the country, as Google did, for example.

If they follow the rules of the game, they will be subject to the scrutiny of civil society and even found accountable in their home countries. That was the case of Microsoft, Yahoo, Cisco and Google, which were requested to give explanations to the US Congress in 2006 due to their unlawful practices in China.[322]

On the other hand, fighting against the laws of the countries (or some of their aspects) leads to deterrent sanctions and even to the loss of administrative licenses. Following our previous example in the US, this approach has led to initiatives such as the bill on the Global Online Freedom Act (GOFA). It was drafted as a code of conduct that would have allowed the US to "guide" US companies on how to behave abroad so as to allegedly respect freedom of expression, the freedom to impart and receive information as well as to combat online censorship. Although considered in 2006 and then unsuccessfully reintroduced in 2007,[323] this "voluntary" code of conduct was reawakened in 2012 [324] and 2013,[325] but has not advanced much yet. In any case, these voluntary codes of conduct have raised concerns among civil society because they are

[321] See https://globalnetworkinitiative.org/participants/index.php (last visited on 17th June 2014).
[322] McMahon, R. (Ed.) and others, *U.S. Internet Providers and the 'Great Firewall of China'*, 23rd February 2011, available at http://www.cfr.org/Internet-policy/us-Internet-providers-great-firewall-china/p9856 (last visited on 16th June 2014).
[323] MacKinnon, R., *Global Online Freedom Act is re-introduced*, 11th January 2007, available at http://rconversation.blogs.com/rconversation/2007/01/global_online_f.html (last visited on 16th June 2014).
[324] Cohn, C. and others, *Global Online Freedom Act 2012 Is An Important Step Forward,* 18th April 2012, available at https://www.eff.org/deeplinks/2012/04/global-online-freedom-act (last visited on 16th June 2014).
[325] US Global Online Freedom Act of 2013, available at http://beta.congress.gov/bill/113th-congress/house-bill/491 (last visited on 27th June 2015).

used by states to sometimes circumvent their positive and negative obligations vis-à-vis international human rights law.

Finally, if foreign companies decided not to conduct business in China as a solution, this would not be enough, as this decision would not be sustainable and competitors may take the opposite decision – to the detriment of a competitive economy. First, even if companies left China, their competitors would replace them, which would undermine the former's economic performance. Secondly, it is unlikely that only foreign companies would exert pressure on the Governing infrastructure of the People's Republic of China. Still, "human rights are good for businesses", as evidenced by the UN's Guiding Principles on Business and Human Rights. However, cases like the already-mentioned cases of Cisco or Google China reflect the need for improvement of both set of rights.[326]

The codes of conduct or guidelines adopted by the international community tend to employ a rather vague and ambiguous wording. That creates legal uncertainty. The fact that they have a non-binding nature makes it inevitable that many human rights breaches will not be prevented. Even if States and other stakeholders gathered together to decide on better practices, there is a risk of perpetuation of abuses in the current international panorama. In a speech given on 12th June 2014 at the International IP Enforcement Summit in London, the US Ambassador to the United Kingdom, Matthew W. Barzun, captured it very well:

> "Companies exist to serve society; society does not exist to serve companies". "In the private sector, we forget about it…"[327]

Within the European Union, there is a lack of evidence-based impact assessments. As an alternative to other non-binding principles or recommendations, civil society and industry gathered together at the Stockholm Internet Forum in 2013 and suggested eight

[326] Global Voices Advocacy, *Human Rights Verdict Could Affect Cisco in China,* 24th April 2013, available at http://advocacy.globalvoicesonline.org/2013/04/24/human-rights-verdict-could-affect-cisco-in-china/; See the letter at http://www.bostoncommonasset.com/news/Investor-Statement-ATS-FINAL.pdf (last visited on 14th June 2014).
[327] Barzun, M. W., speech given at the 2014 International IP Enforcement Summit in London, 12th June 2014, available at https://sslrelay.com/switchnewmedia.com/internationalipenforcementsummit/VOD/Matthew_W_Barzun_Video_Archive.php (last visited on 13th June 2014)

criteria that could be used to assess the legality and effectiveness of "voluntary" measures taken by industry in order to achieve public policy objectives.

First, if the process to conduct such measures is internal, it is more likely the measure will be effective. Second, it is important to ascertain whether the policy objective is initiated or supported by the intermediary to achieve a competitive advantage or to attain economic or societal benefits. Third, the competitiveness of the company is important when considering the overall impact on users. Fourth, the effectiveness and legality of "voluntary" measures need to be assessed vis-à-vis the policy objective pursued. Fifth, their democratic legitimacy is assessed by the law that is being implemented. In the case of China, for instance, this is a very important criterion. In the same vein, the sixth criterion tries to ascertain whether the measures have a different impact depending on the region in which they are implemented. Seventh, the legality and effectiveness of the "voluntary" measures implemented should also be assessed by the responsibility that a company may face in case of a mistaken or arbitrary decision by the intermediary. Additionally, it is important to ascertain the availability of effective redress to users. Finally, the eighth criterion is the collateral damage for liability exceptions.[328]

Despite the criteria described above, there is a lack of a comprehensive and legally binding approach in the European Union, as an opinion of the EESC showed:

> "The success [of] self-regulation depends on several factors: the account they take of the general interest, the transparency of the system, the representativeness and skill of those involved, the existence of assessment and supervision mechanisms and the effectiveness of the monitoring - including sanctions if necessary - and a mutual spirit of partnership between the parties concerned and the public authorities and society in general."[329]

Finally, the EECS pointed out the importance of the 2003 Interinstitutional Agreement on better law making between the Commission, Parliament and Council,[330] whose Article 17 clarifies that "self-regulation" should not be "applicable where fundamental

[328] EDRi, *SIF Unconference: Enforcement through "self-"Regulation – who ever thought this was a good idea?*, 27th May 2013, available at https://edri.org/sif13/ (last visited on 28th June 2015).
[329] The EESC has even developed its own criteria, taken into account experiences of economic actors and input from scholars. Cf. EESC, *Opinion on Self-regulation and co-regulation…, Op. cit.* points 1.6 and 5.21.
[330] European Commission, European Parliament and Council of the European Union, Interinstitutional Agreement on better law making, 2003, available at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2003:321:0001:0005:EN:PDF (last visited on 28th January 2015).

rights or important political options are at stake".[331] Yet, this is not always respected, since many of the measures adopted "voluntarily" by online companies put fundamental rights in conflict with public policy objectives. The EECS notes, however, that the interinstitutional agreement is not binding on third parties[332] – which *inter alia* includes intermediaries.

3. Grounds for companies to restrict Human Rights

Besides the framework described in the precedent section to guide companies to respect human rights online, it is often the case that certain policy objectives of mutual agreement between countries are used as a means to implement measures which may infringe the rule of law and interfere with human rights and freedoms online. Human rights and freedoms can be invoked to justify an Internet control measure, such as blocking[333] – to the detriment of other human rights and freedoms online.

The most common examples relate to child protection, national security, including terrorism, among others. In this section, we examine the role of the intermediaries in the online world and the different approaches China has vis-à-vis the European Union and its Member states, such as the UK, which is a country that has a very developed Internet policy. In fact, the UK experience is an example of how careful we should be when invoking legitimate public interests of protection, because if not dealt with properly, they can lead to indiscriminate censorship without due control.[334]

While the US accused China for spying on the US through undertakings like Huawei,[335] the US intelligence agency, the NSA, has been subject to severe criticism,[336] notably since the Snowden revelations[337] which started on 9th June 2013.[338]

---

[331] Joe McNamee further develops this point. See, for instance, McNamee, J., *Privatised online enforcement series…, Op. cit.*
[332] EESC, *Opinion on Self-regulation and co-regulation…, Op. cit.* point 4.6.
[333] Callanan, C., Gercke, M, De Marco, E., and Dries-Ziekenheiner, H., *Study: Internet blocking, balancing cybercrime responses in democratic societies*, October 2009, p. 133, available at http://www.aconite.com/sites/default/files/Internet_blocking_and_Democracy.pdf (last visited on 28th June 2015).
[334] See, for instance, Moody, G., *Russia And China Both Want To 'Protect Children'…Op. cit.*
[335] U.S. House of Representatives, *Investigative Report on the U.S. National Security Issues Posed by Chinese Telecommunications Companies Huawei and ZTE*, 8th October 2012, available at https://intelligence.house.gov/sites/intelligence.house.gov/files/documents/Huawei-ZTE%20Investigative%20Report%20(FINAL).pdf (last visited on 14th June 2014).

Other countries like India, Australia or the UK have also expressed their concerns on the threats Huawei may cause to national security, especially due to its controversial relationship with the Chinese government.[339] Yet, it is interesting to note that both their governments and companies set up in the aforementioned countries use Huawei's services. For instance, Huawei worked together with TalkTalk in the construction of *Homesafe*[340] in the United Kingdom, which is an opt-out filtering system launched in 2011 to restrict access to certain content, e.g. related to pornography or gambling. As Tim Cushing asked himself,

> "[s]hould UK citizens be concerned their web traffic is being filtered by a company from a filter-heavy nation? Or should they be more concerned that control over content is being handed to a third-party private corporation rather than an independent organization that would be ultimately accountable to Parliament?"[341]

In this section, we address the particular cases of child protection and then national security measures implemented in some of the Member states of the European Union.

Child protection

The Convention on the Rights of the Child is a specific instrument targeted at protecting children's rights. Usually, the Internet is conceived as being a dangerous tool for children. Conversely, potential and tangible benefits are often not given the importance they deserve.

The Internet is a way to exercise the rights of the child. It promotes the right to education in a way that has never been experienced before. The Internet serves as a tool

---

[336] The privacy expert Simon Davies wrote a report analysing the impact of the Snowden revelations. Cf. The Privacy Surgeon (Davies, S., Ed.), *A Crisis of Accountability. A global analysis of the impact of the Snowden revelations*, June 2014, available at http://www.privacysurgeon.org/blog/wp-content/uploads/2014/06/Snowden-final-report-for-publication.pdf (last visited on 14th June 2014).

[337] See the documents that have been leaked so far at https://snowdenarchive.cjfe.org/greenstone/cgi-bin/library.cgi (last visited on 28th June 2015).

[338] The Guardian, *Edward Snowden: the whistleblower behind the NSA surveillance revelations*, available at http://www.theguardian.com/world/2013/jun/09/edward-snowden-nsa-whistleblower-surveillance (last visited on 14th June 2014). There is an independent project in order to track all public documents related to the NSA: https://www.nsa-observer.net/ (last visited on 22nd January 2015).

[339] U.S. House of Representatives, *Op. cit.* pp. 25 and 26

[340] Cf. http://www.talktalk.co.uk/security/homesafe-demo.html; http://www.huawei.com/ilink/en/success-story/HW_196215 (last visited on 14th June 2014).

[341] Cushing, T., *UK's Anti-Porn Filtering Being Handled By A Chinese Company*, 25th July 2013, available at https://www.techdirt.com/articles/20130725/20042323953/uks-anti-porn-filtering-being-handled-chinese-company.shtml (last visited on 14th June 2014).

to spread knowledge, to promote the development of the personality of the child, to encourage self-determination and to help the child to become more mature.

Most of the grounds for setting internet control measures to purportedly protect children can be considered as legitimate by default. Concerns arise in order to prevent online bullying, child pornography, hate speech, defamation, harassment, intimidation or discrimination based, for instance, on race or sex. Nonetheless, the approach adopted by the vast majority of countries and intermediaries is unbalanced. In the words of the former Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank LaRue, risks threatening children on the Internet are "overstated and used as an excuse for unduly restricting the rights of both adults and children", such as freedom of expression. [342]

"Widespread restrictions on the use of digital communications and censorship are not only unacceptable but also ineffective solutions to these concerns".[343] Those restrictions are usually based on "vague" and "broad" conceptions of what harmful information is as well as on a "tacit acceptance of authoritarian attitudes". [344] Additionally, differences in age are usually not taken into account.[345] Thus, the concept of "children" includes individuals from the day they are born until their last years as a teenager, usually 16, 18 or 21. As the former UN Special Rapporteur argued, however,

> "[c]hildren's freedom of expression does not —and cannot —start when children become capable of expressing their views autonomously or become teenagers; they cannot be expected to develop as autonomous beings and participants in society at the magical age of 18 years without having had the opportunity beforehand."[346]

Freedom of expression online is an obvious example of clear breaches that have been implemented in our society purportedly for protecting children. In general, measures placed by the State do not take into consideration the different levels of realisation of the child as he or she grows older, 'paternalistic attitudes' or underestimate the ability of the child to make choices or express himself or herself. [347] The same concerns can be

[342] Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion, 21st August 2014, para. 3, available at https://www.crin.org/sites/default/files/freedomofexpression_2.pdf (last visited on 27th June 2015).
[343] *Ibid*, para. 4
[344] *Ibid*, para. 3.
[345] *Ibid*. 12.
[346] *Ibid.*
[347] *Ibid*, para. 34.

raised as regards measures applied by the ISP on a voluntary basis or encouraged by a government.

It is interesting to note how China considers child protection in terms of policy and the measures put in place in the country to tackle the issues surrounding the protection of children. According to the Information Office of the State Council of the People's Republic of China,

> "The state guarantees online safety for minors. Minors have become China's biggest online group. By the end of 2009, a third of the country's 384 million Internet users were minors. The Internet is playing an increasingly important role in the development of minors. Meanwhile, online pornographic, illegal and harmful information is seriously damaging the physical and psychological health of young people, and this has become recognized as a prominent issue of public concern. The Chinese government attaches great importance to online safety for minors, and has always prioritized the protection of minors in the overall work of Internet information security programs. The Law of the People's Republic of China on the Protection of Minors[348] stipulates that the state shall take measures to prevent minors from overindulging in the Internet; prohibit any organization or individual from producing, selling, renting or providing by other means electronic publications and Internet information containing pornography, violence, murder, terror, gambling or other contents harmful to minors. The state encourages research and development of Internet tools that are conducive to the online protection of minors, as well as Internet products and services suitable for minors. Families, schools and all other social units shall work together to protect minors online and create a healthy online environment for the development of minors. The Chinese government will actively push forward the "Mothers' Education Program" to help parents guide their children in using the Internet correctly."[349]

Whereas in China online intermediaries (mainly ISPs) face liability if they do not take measures to protect children, the EU and its Member States have a generally more comprehensive and just system. Yet, the EU is failing to address this legitimate interest with the most effective technology.[350] Put simply, the EU system is not exempt from criticism either, as it has been criticised for not taking an evidence-based approach in policy-making.[351] This is perhaps best illustrated by the almost complete absence (until

[348] Law of the People's Republic of China on the Protection of Minors, 26th October 2012, available at http://www.lawinfochina.com/display.aspx?id=12626&lib=law&SearchKeyword=protection%20minors&SearchCKeyword= (last visited on 28th January 2015). For instance, its Article 11 calls on parents to provide education to their children so as to fight against "internet addiction".
[349] Information Office of the State Council of the People's Republic of China, *Op. cit.*
[350] Alexandra Chernyavskaya and Professor Sara Livingston provided a guide which reflects an overview of the organisations which are working to protect children online. Cf. Chernyavskaya, A. and Livingstone, S., *Children's safety on the internet: a guide to stakeholders*, London School of Economics and Political Science, Media Policy Project Blog, 31st March 2015, available at http://blogs.lse.ac.uk/mediapolicyproject/2015/03/31/childrens-safety-on-the-internet-a-guide-to-stakeholders/ (last visited on 28th June 2015).
[351] See, for instance, Chernyavskaya, A., *Evidence-based policymaking for provision of children's rights online*, London School of Economics and Political Science, Media Policy Project Blog, 24th June 2015,

recently) of statistics being collected – or requests for statistics to be collected – by hotlines set up to receive reports of child abuse online and funded by the European Commission.[352]

National security

As Edward Foster stated in 1951, "[w]e are willing enough to praise freedom when she is safely tucked away in the past and cannot be a nuisance. In the present, amidst dangers whose outcome we cannot foresee, we get nervous about her, and admit censorship."[353] But when should confidentiality give way to security?[354]

There are several examples within the European Union of Member states which have implemented greater restrictions on fundamental rights and freedoms online for the purposes of preserving national security, in general, or fighting against terrorism, in particular.

Terrorism has become one of the biggest problems faced by mankind especially in recent times. According to Criminal Law Specialist Lamarca Pérez, antiterrorism legislation is where democratic states greater show an authoritarian tendency that seriously violates the efficiency of individual guarantees. Antiterrorism laws somewhat deny the rule of law.[355] In order to exemplify this ground for restricting human rights and fundamental freedoms online through privatised enforcement, we chose France.

---

available at http://blogs.lse.ac.uk/mediapolicyproject/2015/06/24/evidence-based-policymaking-for-provision-of-childrens-rights-online/ (last visited on 28th June 2015).

[352] See, for instance, the lack of reliability of the statistics provided by the UK Internet Watch Foundation in its 2007 and 2008 annual reports. Cf. Libertus, *Web sites: U.K. Internet Watch Foundation ("IWF") 2008 & 2007 statistics, in* Statistics Laundering: false and fantastic figures, 2009, available at http://libertus.net/censor/resources/statistics-laundering.html#iwfstats (last visited on 4th August 2015).

[353] Kovarovic., K., *When the Nation Springs a [Wiki]Leak: The 'National Security' Attack on Free Speech*, Touro International Law Review, Vol. 14, Nº. 2, 14th May 2011, available at http://ssrn.com/abstract=1841923 (last visited on 13th July 2015).

[354] A.D. Moore tries to make a balance between privacy and security "while maintaining accountability". In order to exemplify its theory, he includes a table which "measures privacy interests across several dimensions". See, Moore, A.D., *Privacy, Security, and Government Surveillance: WikiLeaks and the new Accountability*, Public Affairs Quaterly, Vol. 25, Nº 2, April 2011, pp. 148-152, available at https://www.law.upenn.edu/institutes/cerl/conferences/ethicsofsecrecy/papers/reading/Moore.pdf (last visited on 13th July 2015).

[355] Lamarca Pérez, C. et al, Derecho Penal. Parte especial, Ed. Colex, 4th Edition, Madrid, 2008, p. 739.

Terrorism is being used as a reason for greater monitoring on (and off) line. Fighting against terrorist attacks is a valid and legitimate interest to protect. However, such public interest cannot be an excuse for blanket restrictions on our human rights and fundamental freedoms.

At the beginning of January 2015, several people were killed at the headquarters of the satiric newspaper 'Charlie Hebdo in Paris. After this tragic episode, the French government proposed a package of measures, further restricting privacy, increasing control measures on the Internet, enforcing communications data retention provisions and passenger name record storage for profiling purposes, among others.[356]

We are of the opinion that such approach is not appropriate. As Hecker, an expert from the *Institut Français des Relations Internationales*, recalled, the last anti-terrorist law enacted in France before the "Loi au Renseignement" dated back from November 2014 and that other counter-terrorism law did not prove helpful.[357] In fact, from 2001 to date, France adopted several pieces of legislation to counter terrorism actions that included provisions related to the Internet. In addition, France had been retaining telecommunications and Passenger Name Records (PNR) for a long time now, but still failed to prevent the 'Charlie Hebdo' tragedy.

The first terrorist law France enacted regarding the Internet dates back to 15th November 2001,[358] which followed the 11 September terrorist attacks in the US. . It authorised the use of surveillance technology and data retention obligations for telecommunication operators. [359] Moreover, it contained provisions reforming the French Criminal Procedural Code.[360] For instance, since the entry into force of the anti-terrorist law,

[356] See the official measures envisaged: Gouvernement Français, *#Antiterrorisme : Manuel Valls annonce des mesures exceptionnelles*, 21st January 2015, available at http://www.gouvernement.fr/antiterrorisme-manuel-valls-annonce-des-mesures-exceptionnelles (last visited on 28th January 2015).
[357] Hecker, M., *La menace terroriste en France*, Institut Français des Relations Internationales, 9th January 2015, interview available at http://www.ifri.org/fr/publications/editoriaux/actuelles-de-lifri/jihad-syrie-irak-un-defi-france (last visited on 11th January 2015).
[358] Loi [française] n° 2001-1062 du 15 novembre 2001 relative à la sécurité quotidienne, available at http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000222052&dateTexte=&categorieLien=id (last visited on 28th January 2015).
[359] Comité d'Experts sur le terrorisme, *Profils nationaux relatifs à la capacité de lutte contre le terrorisme: France*, Council of Europe, September 2013, p.3, available at http://www.coe.int/t/dlapil/codexter/Country%20Profiles/Profiles%202013%20France_FR.pdf (last visited on 28th January 2015).
[360] "Code de procédure pénale français", available at

Article 230-1 of the French Criminal Procedural Code started allowing the public prosecutor and investigating and trial judges to order the use of national secret defence technical means to decrypt encrypted messages. This power has been extended to certain policy officers as of 14th November 2014.[361]

On 29th August 2002, another law was enacted to merge several databases in order to preserve "internal security". It is known as "LOPSI".[362] One year later, on 18th March 2003, the LOPSI was promulgated[363] to extend the obligation on operators to retain and disclose their communication data. On 21st June 2004, France adopted a law on trust in the Digital economy, according to which the police could incorporate devices like cameras or microphones in vehicles and private homes without notifying or providing a justification to the owner of this invasion of his or her privacy.[364]

On 23rd January 2006, France adopted another law.[365] It was aimed at intensifying sanctions, the control of the Internet and the interception of communications, such as phone communications. On 22nd January 2009, a decree[366] developed this law so as to reinforce the video-surveillance measures which were in force after the 2006 legislation.

---

http://www.legifrance.gouv.fr/affichCode.do;jsessionid=56FC6E2ACAD19750B5D2F073F07E3AC0.tpdila16v_3?cidTexte=LEGITEXT000006071154&dateTexte=20150804 (last visited on 4th August 2015).

[361] According to the latest reform of this Article, "*officiers de police judiciaire*" can be granted authorisation by the public prosecutor or a judge to order the decryption of encrypted communications, resorting to national defence mechanisms which are considered as state secrets.

[362] Loi [française] n° 2002-1094 du 29 août 2002 d'orientation et de programmation pour la sécurité intérieure, available at http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000780288 (last visited on 28th January 2015).

[363] Loi [française] n° 2003-239 du 18 mars 2003 pour la sécurité intérieure, available at http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=LEGITEXT000005634107&dateTexte=vig (last visited on 28th January 2015).

[364] Loi [française] n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique, available athttp://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000801164&dateTexte=&categorieLien=id (last visited on 28th January 2015).

[365] Loi [française] n° 2006-64 du 23 janvier 2006 relative à la lutte contre le terrorisme et portant dispositions diverses relatives à la sécurité et aux contrôles frontaliers, available at http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000454124&dateTexte=&categorieLien=id (last visited on 28th January 2015).

[366] Décret [français] n° 2009-86 du 22 janvier 2009 modifiant le décret n° 96-926 du 17 octobre 1996 relatif à la vidéosurveillance, available at http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000020146614&dateTexte=&categorieLien=idblank (last visited on 28th January 2015).

On 14th March 2011, the LOPSI was updated.[367] This reform included provisions that contributed to Internet censorship, extended police databases, introduced body scanners and enhanced the utilisation of surveillance cameras.[368]

On 13th November 2014, France adopted another law by accelerated procedure [369] so as to reinforce the existing provisions to fight against terrorism.[370] France strengthened Internet control by *inter alia* allowing administrative authorities (such as the police) to require ISPs to block certain content on the basis of a public interest reason without a court order. Due to the concerns raised to freedom to receive and information, freedom of movement or freedom of expression,[371] civil society organisations like La Quadrature du Net launched a campaign to raise public awareness on the dangers of this French law[372], but did not prevent its adoption. The "Loi au renseignement" suffered the same fate. On 24th June 2015, it was adopted by the National legislative Assembly. However,, on 25th June 2015, more than sixty members of parliament and the President of the Senate appealed it before the French Constitutional Court (the '*Conseil constitutionnel*'), [373]although without success.[374] The aforementioned civil society organisation announced plans to challenge the law before the ECtHR.[375]

[367] Loi [française] n° 2011-267 du 14 mars 2011 d'orientation et de programmation pour la performance de la sécurité intérieure (LOPSI II), available at http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000023707312&dateTexte=&categorieLien=id (last visited on 28th January 2015).
[368] Fiedler, K., *Patriot Act à la française: Braucht Frankreich weitere Überwachungsmaßnahmen?*, 26th January 2015, available at https://netzpolitik.org/2015/franzoesischer-patriot-act-ueberwachungsmassnahmen/ (last visited on 28th January 2015).
[369] Reporteurs Sans Frontières, *La liberté d'information menacée au nom de l'urgence terroriste*, 18th July 2014, available at http://fr.rsf.org/france-la-liberte-d-information-menacee-18-07-2014,46659.html (last visited on 8th January 2015).
[370] Loi [française] n° 2014-1353 du 13 novembre 2014 renforçant les dispositions relatives à la lutte contre le terrorisme, available at http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000029754374&dateTexte=&categorieLien=id (last visited on 8th January 2015).
[371] Cf. *Ibid*, Articles 1, 5, 9 and 12.
[372] See their campaign at https://presumes-terroristes.fr/ (last visited on 28th June 2015).
[373] Projet de loi relatif au renseignement, Legislative dossier, France, available at http://www.assemblee-nationale.fr/14/dossiers/renseignement.asp (last visited on 28th June 2015).
[374] Only three articles (or some references contained therein) were declared unconstitutional by the French Constitutional Court. Cf. French Constitutional Court, ruling No. 2015-713 DC of 23rd July 2015, available at http://www.conseil-constitutionnel.fr/conseil-constitutionnel/francais/les-decisions/acces-par-date/decisions-depuis-1959/2015/2015-713-dc/decision-n-2015-713-dc-du-23-juillet-2015.144138.html (last visited on 4th August 2015).
[375] La Quadrature du Net, *Publication d'un mémoire citoyen au Conseil Constitutionnel contre la loi Renseignement !*, 23rd June 2015, available at http://www.laquadrature.net/fr/publication-dun-memoire-citoyen-au-conseil-constitutionnel-contre-la-loi-renseignement (last visited on 5th August 2015).

At the EU level, reactions appeared very quickly as well. Right after the terrorist attack, the Ministers of Internal Affairs of Germany, Austria, Belgium, Denmark, Spain, Italy, Latvia, the Netherlands, Poland, the United Kingdom and Sweden joined the French Minister of Interior and issued a declaration on 11th January 2015. They asked for legislation on passenger name record retention and profilng, more telecommunications data retention and an increase of the control of the Internet.[376] While they foresaw measures to fight against terrorism and radicalisation online, they considered it appropriate to create a non-defined forum of internet ISPs, while "scrupulously" observing fundamental freedoms and respecting the law.[377] However, there are not clear rules in the laws of the Member states or the EU itself to counterbalance the obligation to preserve a legitimate aim of public interest. Looking at the expansive policing measures being demanded of these same companies by the US draft Cybersecurity Information Sharing Act[378], the notion that the "voluntary" forum will respect the spirit and letter of, for example, Article 52 of the EU Charter of Fundamental Rights, is far from clear.

Similarly, the European Commission also reacted by foreseeing counter-terrorist actions for the near future in terms of EU policy.[379] On 28th April 2015, the European Commission launched a European Agenda on Security.[380] Among its priorities, the Commission re-stated the goal already mentioned by the joint-statement of the Ministers of the Interior: the creation of "an EU Forum with IT companies to help counter terrorist propaganda and addressing concerns about new encryption technologies".[381] In other words, a forum to implement "voluntary" measures to tackle terrorism online, without any accountability in case companies over- or under-implement the measures they are

[376] Meyer, D., *EU's response to free speech killings? More internet censorship*, Gigaom, 11th January 2015, https://gigaom.com/2015/01/11/eu-response-to-free-speech-killings-more-internet-censorship/ (last visited on 11th January 2015).
[377] Cazeneuve, B. (coord.), Joint statement, Paris, 11th January 2015, available at https://www.bmi.bund.de/SharedDocs/Downloads/DE/Kurzmeldungen/gemeinsame-erklaerung.pdf?__blob=publicationFile (last visited on 29th June 2015).
[378] US Cybersecurity Information Sharing Act of 2015, S.754 , 114th Congress (2015-2016), available at https://www.congress.gov/bill/114th-congress/senate-bill/754 (last visited on 4th July 2015).
[379] European Commission, Press Release - *La lutte contre le terrorisme au niveau européen : présentation des actions, mesures et initiatives de la Commission européenne*, 11th January 2015, available at http://europa.eu/rapid/press-release_MEMO-15-3140_fr.htm (last visited on 11th January 2015).
[380] European Commission, *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: The European Agenda on Security*, COM(2015) 185 final, Strasbourg, 28th April 2015, available at http://ec.europa.eu/dgs/home-affairs/e-library/documents/basic-documents/docs/eu_agenda_on_security_en.pdf (last visited on 29th June 2015).
[381] *Ibid*, p. 16.

encouraged to take, such as blocking, filtering of or taking down content or informal data sharing.[382]

In sum, the situation in the European Union counts with more guarantees for human rights and fundamental freedoms online than in China. Nevertheless, this does not mean that the EU system is not exempt of criticism. On the contrary, measures undertaken and the grounds that justify them are not that different.

V. CONCLUSION

While providing an overview of the Internet situation in China in comparison with the European Union and some of its Member states, we sought to demonstrate the situation in China vis-à-vis human rights restrictions online is not that different from the situation in the European Union. The EU and its Member States have more protective legal and political frameworks. The EU has democracy foundations. China does not. Yet, there are five main reasons which demonstrate there are more similarities than what one may think.

First, both Parties have different Internet governance models. However, both models can be criticised. In addition, the different models are leading to similar policy-making decisions.

One the one hand, China defends national sovereignty over the Internet (interstate model) and countries like EU Member States, formally support a free, open and bottom-up multistakeholder system (multistakeholderism). Yet, multistakeholderism is leading to a set of irregularities.

China's vision of the Internet is that each nation must retain the power to control Internet policies. Consequently, no other country or international actor can undermine its sovereignty, even within a context of international cooperation. China acknowledges that it is not possible to isolate itself. Hence, it uses all international mechanisms to its benefit, as any international actor would do. It fosters further '*democratisation*' in the

[382] Fiedler, K., *EU Commission set to re-brand the failed CleanIT project*, 3rd June 2015, available at https://edri.org/eu-commission-rebrand-failed-cleanit-project/ (last visited on 29th June 2015).

decision process so it can ensure it is going to be heard and be able to persuade others. That trend has been already tested in NETmundial, where China submitted its view on how the Internet should be regulated, together with Russia, Tajikistan and Uzbekistan.

Inside the EU, the nature of the power over the Internet is changing. In fact, the European Union is living in an era in which all multistakeholders wish to advocate what is best for them or for the interests they represent.

On the other hand, differences related to how China and the EU wish to govern the Internet have led to similar outcomes in terms of Internet regulation. In fact, there is a tendency in Europe to implement mechanisms of control outside the rule of law with similar effects although justified on public interest grounds. How effectively human rights online can be protected by all stakeholders while pursuing other public policies is a challenge that EU is facing and, as we have seen, not addressing very well.

Second, we acknowledged that China has an innumerable number of Internet users as compared to the total number of Internet users. However, Internet penetration is not uniform. In the European Union, Internet penetration is still a problem. As stated elsewhere, while "100% of Europeans now have access to broadband",[383] out of all EU citizens, 20% "have never used the internet. Rural areas are not provided with a high speed broadband, and given that nearly half of the Europeans lack sufficient information and communications technology (ICT) skills, it is obvious that access is not equivalent to broadband subscription or actual usage. Accordingly, the European Commission [itself] recognises there is still room for improvement."[384]

Third, the "Internet's open architecture is under attack from multiple directions".[385] As Kulesza puts it, the Internet has "changed more than just the perception of human rights", but it has also changed the role of governments and companies.[386] China mainly deploys three forms of Internet control, namely censorship, arbitrary intermediary

[383] European Commission, *Scoreboard 2014 - Progress Report Digital Agenda Targets 2014*, 28th May 2014, available at https://ec.europa.eu/digital-agenda/en/news/scoreboard-2014-progress-report-digital-agenda-targets-2014 (last visited on 1st July 2015).
[384] Fernández Pérez, M., *EC's Scoreboard 2014…, Op. cit.*
[385] Landau, S., Surveillance or Security? The Risks Posed by New Wiretapping Technologies, Massachusetts Institute of Technology, 2010, p. 34
[386] Kulesza, J., *Op. cit.*, p. 2.

intervention and self-censorship. In the European Union, there are many countries and companies whose measures are leading to control the Internet in a non-proportionate, untested way. The end product is more similar than what would have seemed likely just a few years ago.

Fourth, the Internet facilitates the enhancement of human rights and freedoms online. Notwithstanding its benefits, the Internet is posing many threats to human rights, such as freedom of expression and the right to privacy, resulting in loss of trust in the system.[387] This is a clear reality in China. In the European Union, restrictions to human rights are taking place and growing at a precipitous rate.

Fifth, the greatest threat to human rights and fundamental freedoms online in both China and the EU come from the role of intermediaries. While in China, intermediaries face liability, in Europe the legal regime is more protective. However, there is increasing pressure to change this.[388] This is an inherent threat, as the Internet is a public space that is privately owned. Companies do not have the same obligations to respect human rights as States have. Europe is not an exception. More and more companies are being "encouraged" to take measures which bypass the rule of law. Power without responsibility is never good and never sustainable.

Ultimately, the real impact international practices have on the Chinese Internet policies is yet to be seen. So far, it seems more likely that in the near future China will be of inspiration to many countries than the other way around in the sense that instead of promoting and protecting digital rights, more challenges will arise. Overall, China may

[387] MacDonald, R., Ben-Avie, J. and Carrion, F., Internet freedom and the right to private life, protection of personal data and due process of law, Report drafted by Access for the Council of Europe, MCM(2013)008, 2013, p. 5.

[388] See, for instance, Section 3(3) of the Digital Single Market Communication of the European Commission or the European Parliament's draft report on terrorist radicalisation and recruitment online. Cf. Respectively, European Commission, *A Digital Single Market Strategy for Europe* , Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, COM(2015) 192 final, Brussels, 6th May 2015, available at http://ec.europa.eu/priorities/digital-single-market/docs/dsm-communication_en.pdf (last visited on 5th August 2015) and European Parliament (rapporteur Dati, R.,), Draft report *on prevention of radicalisation and recruitment of European citizens by terrorist organisations*, 2015/2063(INI), Committee on Civil Liberties, Justice and Home Affairs, 1st June 2015, available at http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-%2f%2fEP%2f%2fNONSGML%2bCOMPARL%2bPE-551.967%2b01%2bDOC%2bPDF%2bV0%2f%2fEN (last visited on 5th August 2015).

not be the greatest example of promotion and protection of civil rights and liberties in the digital world, but can Europe plead not guilty?

BIBLIOGRAPHY

Academic articles

Anonymous, *China and the Internet*, Harvard International review, Summer 2009, Vol. 31 Issue 2

Arsène, S., *Online discussions in China. China Perspectives, French Center for Research on Contemporary China*, 2008, available at https://hal.archives-ouvertes.fr/hal-00773584/document

Arsène, S., *Protester sur le web chinois (1994-2011), Le Temps des médias*, 2012, available at https://hal.archives-ouvertes.fr/hal-00773738/document

Arsène, S., *The impact of China on global Internet governance in an era of privatized control*, Chinese Internet Research Conference, May 2012, Los Angeles, United States, available at https://hal.inria.fr/file/index/docid/704196/filename/circ_14mai.pdf

Bambauer, D.E., *Consider the Censor,* Wake Forest Journal of Law & Policy, Forthcoming; Brooklyn Law School, Legal Studies Paper Nº 218, p.4, available at http://ssrn.com/abstract=1757890

Broude, Tomer and Hestermeyer, Holger P., *The First Condition of Progress? Freedom of Speech and the Limits of International Trade Law*, 5th May 2013, Virginia Journal of International Law, available at http://ssrn.com/abstract=2260969

Callanan, C., Gercke, M, De Marco, E., and Dries-Ziekenheiner, H., *Study: Internet blocking, balancing cybercrime responses in democratic societies*, October 2009, available at http://www.aconite.com/sites/default/files/Internet_blocking_and_Democracy.pdf

Clarke, D. C., *Empirical Research Into the Chinese Judicial System*, 15th July 2003, available at http://ssrn.com/abstract=412660

Conley, N., *The Chinese Communist Party's New Comrade: Yahoo's Collaboration with the Chinese Government in Jailing a Chinese Journalist and Yahoo's Possible Liability Under the Alien Torts Claim Act*, 15th June 2006, available at http://ssrn.com/abstract=1420373

ECFR, *China's Expanding Cyberspace*, June 2014, available at http://www.ecfr.eu/page/-/ChinaAnalysisEng_June2014.pdf

ECFR, *China 3.0*, November 2012, available at http://www.ecfr.eu/page/-/ECFR66_CHINA_30_final.pdf

Erixon, F., Hindley, B. and Lee-Makiyama, H., *Protectionism Online: Internet Censorship and International Trade Law*, available at http://www.ecipe.org/media/publication_pdfs/protectionism-online-Internet-censorship-and-international-trade-law.pdf

Fu, Y. and Peerenboom, R., *A New Analytical Framework for Understanding and Promoting Judicial Independence in China*, 1st February 2009, available at http://ssrn.com/abstract=1336069

Gao, H.S., *Google's China Problem: A Case Study on Trade, Technology and Human Rights Under the GATS*, Asian Journal of WTO & International Health Law and Policy (AJWH), Vol. 6, 2011, available at http://ssrn.com/abstract=1976611

García-Bolívar, *Lack of judicial independence and its impact on transnational and international litigation,* Law and Business Review of the Americas 18.1, Winter 2012

Garot, M.-J., *El poder judicial en China: ¿independiente y eficaz?,* InDret, Vol. 2, 2009, May 2009, available at http://www.indret.com/pdf/629_es.pdf

Green, M.J. and Szechenyi, N., *Power and Order in Asia. A Survey of Regional Expectations, Center for Strategic and International Studies*, 5th June 2014, available at http://csis.org/files/publication/140605_Green_PowerandOrder_WEB.pdf

Greenlee, M.J., *A King Who Devours His People: Jiang Zemin and the Falun Gong Crackdown: A Bibliography*, International Journal of Legal Information: Vol. 34: Iss. 3, Article 9, January 2006, available at http://scholarship.law.cornell.edu/cgi/viewcontent.cgi?article=1074&context=ijli

Hachigian, N., Chen, W. and Beddor,C., *China's New Engagement in the International System. In the ring, but punching below its weight,* Center for American Progress, November 2009, available at http://www.americanprogress.org/wp-content/uploads/issues/2009/11/pdf/chinas_new_engagement.pdf

Herold, D.H., *An Inter-nation-al Internet: China's contribution to global Internet governance?*, 5th September 2011, available at http://ssrn.com/abstract=1922725

Institut Français des Relations Internationales (Nocetti, J., coord.), *Internet: une gouvernance inachevée, Politique étrangère*, n° 4, hiver 2014-2015.

Kleinwächter, W, *Beyond ICANN Vs ITU? How WSIS Tries to Enter the New Territory of Internet Governance*, 2004 Gazette 66 (3-4): 233–51

Kovarovic., K.,*When the Nation Springs a [Wiki]Leak: The 'National Security' Attack on Free Speech*, Touro International Law Review, Vol. 14, Nº. 2, 14th May 2011, available at http://ssrn.com/abstract=1841923

Kulesza, J., *Protecting Human Rights Online -- An Obligation of Due Diligence*, Jean Monnet Working Paper 24/14, 2014, available at http://www.jeanmonnetprogram.org/papers/14/documents/JMWP24Kulesza.pdf

Lee, J-A., Liu, C-Y. and Li, W., *Searching for Internet Freedom in China: A Case Study on Google's China Experience*, 1st April 2013, Cardozo Arts & Entertainment Law Journal, Vol. 31, No. 2, 2013, available at http://ssrn.com/abstract=2243205

Liebman, B. and Wu., T., *China's Network Justice*, Columbia Public Law Research Paper No. 07-143, 9th January 2007, available at http://ssrn.com/abstract=956310

Ling, Y., *Upholding Free Speech and Privacy Online: A Legal-Based and Market-Based Approach for Internet Companies in China*, 6 May 2010, Santa Clara Computer and High Technology Law Journal, available at http://ssrn.com/abstract=1604173

Lubman, S., *Looking for law in China*, Columbia Journal of Asian Law, Spring/Fall

McMahon, R. (Ed.) and others, *U.S. Internet Providers and the 'Great Firewall of China'*, 23rd February 2011, available at http://www.cfr.org/Internet-policy/us-Internet-providers-great-firewall-china/p9856#p4

McNamee, J., *Should Reporting-based Human Rights Treaties Be Considered "Binding International law"?*, University of Kent, Brussels, 1st September 2006, available at http://www.ibrarian.net/navon/paper/Should_Reporting_based_Human_Rights_Treaties_Be_C.pdf?paperid=8325925

Minzner, C.F., *China's Turn Against Law*, American Journal of Comparative Law, 2011; Washington University in St. Louis Legal Studies Research Paper No. 11-03-01, available at http://ssrn.com/abstract=1767455

Moore, A.D., *Privacy, Security, and Government Surveillance: WikiLeaks and the new Accountability*, Public Affairs Quaterly, Vol. 25, Nº 2, April 2011, available at https://www.law.upenn.edu/institutes/cerl/conferences/ethicsofsecrecy/papers/reading/Moore.pdf

Musielak, *L.T., "Google-ing" China: An ethical analysis of Google's censorship activities in the People's Republic*, 2010, available at http://snl.depaul.edu/writing/Googleing%20China.pdf

Palfrey, J. G., *Local Nets on a Global Network: Filtering and the Internet Governance Problem. THE GLOBAL FLOW OF INFORMATION*, Harvard Law School, Public Law & Legal Theory Paper Series, Working Paper No. 10-41, available at http://ssrn.com/abstract=1655006

Peerenboom, R., *Between Global Norms and Domestic Realities: Judicial Reforms in China*, 8th May 2009, available at http://ssrn.com/abstract=1401232

Peerenboom, R., *Fly High the Banner of Socialist Rule of Law with Chinese Characteristics! What Does the 4th Plenum Decision Mean for Legal Reforms in China?*, 6th November 2014, available at http://ssrn.com/abstract=2519917

Peerenboom, R., *Judicial Independence in China: Common Myths and Unfounded Assumptions*, La Trobe Law School Legal Studies Research Paper No. 2008/11, available at http://ssrn.com/abstract=1283179

Subba, B.B., *18th CPC Central Committee Fourth Plenum: Rule of Law with Chinese Characteristics*, Institute of Chinese Studies, No. 22, Delhi, November 2014, available at http://www.icsin.org/ICS/ICSAnalysispdf/32.pdf

Wagner, B., *Calling a Bluff? Internet Governance Poker Heats up*, 9th April 2014, available at http://cgcsblog.asc.upenn.edu/2014/04/09/calling-a-bluff-Internet-governance-poker-heats-up/?utm_source=feedburner&utm_medium=email&utm_campaign=Feed:+CGCSMediaWire+%28The+Center+for+Global+Communication+Studies+%28CGCS%29%29

Wu, T., *A proposal for Network Neutrality*, June 2002, available at http://www.timwu.org/OriginalNNProposal.pdf (last visited on 21st June 2015).

Ye, A., and Song, Y., *Justice, efficiency and the new Civil Procedure Law,* China Law & Practice, Nov/Dec 2012

Zhang, X., *A law unto themselves: the Chinese government has acknowledged that corruption in the judiciary is a serious problem,* Hong Kong Lawyer, Vol. Mar, No. 1, Article no. 4, 1998, available at http://ssrn.com/abstract=1810187

Blog articles

Abrams, S., *China's Internet Cafes Respond to ID Check Rules*, available at http://www.chinahearsay.com/china-Internet-cafes-respond-id-check-rules/

AccessNow, *Policy Brief: Access' position on zero rating schemes*, 2015, available at https://s3.amazonaws.com/access.3cdn.net/d812d59f706c3e8a75_w0m6iipn5.pdf

Access and EDRi, *Net neutrality – building on success*, available at https://www.accessnow.org/blog/2015/06/01/net-neutrality-building-on-success

ACLU, *What is Censorship?*, 30th August 2006, available at https://www.aclu.org/free-speech/what-censorship

Bell, I., *The Open Debate on Chinese Internet Proliferation*, 22 July 2009, http://www.ianbell.com/2009/07/22/the-open-debate-on-chinese-Internet-proliferation/

Bonaventure, O., *DNS injection can pollute the entire Internet*, 30th August 2012, available at http://perso.uclouvain.be/olivier.bonaventure/blog/html/2012/08/30/dns_injection_can_pollute_the_entire_internet.html

Brown, D., and Kaspar, L., *Everything you need to know about the WSIS+10 review*, Association for Progressive Communications News, 28th January 2015, available at https://www.apc.org/en/news/everything-you-need-know-about-wsis10-review

Chernyavskaya, A., *Evidence-based policymaking for provision of children's rights online*, London School of Economics and Political Science, Media Policy Project Blog, 24th June 2015, available at http://blogs.lse.ac.uk/mediapolicyproject/2015/06/24/evidence-based-policymaking-for-provision-of-childrens-rights-online/

Chernyavskaya, A. and Livingstone, S., *Children's safety on the internet: a guide to stakeholders*, London School of Economics and Political Science, Media Policy Project Blog, 31st March 2015, available at http://blogs.lse.ac.uk/mediapolicyproject/2015/03/31/childrens-safety-on-the-internet-a-guide-to-stakeholders/

Cohn, C. and others, *Global Online Freedom Act 2012 Is An Important Step Forward,* 18th April 2012, available at https://www.eff.org/deeplinks/2012/04/global-online-freedom-act

Connaught Summer Institute, *Internet Censorship Lab*, 26th July 2013, available at http://www.cs.stonybrook.edu/~phillipa/icl_slides.pdf

Cushing, T., *UK's Anti-Porn Filtering Being Handled By A Chinese Company*, 25th July 2013, available at https://www.techdirt.com/articles/20130725/20042323953/uks-anti-porn-filtering-being-handled-chinese-company.shtml

Daxue Consulting, *Overview of the E-commerce Market in China*, 2013, available at http://daxueconsulting.com/overview-of-the-e-commerce-market-in-china/

DelPiano, P., *Censorhip, self-censorship and freedom of the press in Europe*, Europia Magazine, 13th February 2015, available at http://www.eutopiamagazine.eu/en/patrizia-delpiano/issue/censorship-self-censorship-and-freedom-press-europe-0

EDRi, *Failure Of "Licenses For Europe",* 20th November 2013, available at https://edri.org/failure-of-licenses-for-europe/

EDRi, *Net neutrality*, The EDRi papers, Issue 08, 22nd December 2013, available at https://edri.org/files/paper08_netneutrality.pdf

EDRi, *How the Internet Works. A guide for policy-makers*, The EDRi papers, Issue 03, 23rd January 2012, available at http://www.edri.org/files/2012EDRiPapers/how_the_internet_works.pdf

EDRi, *SIF Unconference: Enforcement through "self-"Regulation – who ever thought this was a good idea?*, 27th May 2013, available at https://edri.org/sif13/

EFF, *Cisco and Abuses of Human Rights in China: Part 1,* 8th July 2011, available at https://www.eff.org/deeplinks/2011/07/eff-urges-microsoft-and-cisco-to-reconsider-china

Fernández Pérez, M., *EC's Scoreboard 2014: Broadband access improved, challenges remain*, 4th June 2014, available at http://edri.org/ecs-scoreboard-2014-broadband-access-improved-challenges-remain/

Fernández Pérez, M., *Net Neutrality: document pool II*, 15th April 2015, available at https://edri.org/net-neutrality-document-pool-2/

Fernández Pérez, M., *Spain: social media to be censored? "Not everything is appropriate"*, 21st May 2014, http://edri.org/spain-social-media-to-be-censored-not-everything-is-appropriate/

Fernández Pérez, M., *Spain: Why you should care about the Citizens' Security Bill*, 30th July 2014, available at https://edri.org/spain-citizens-security-bill/

Fernández Pérez, M. and Massé, E., *Spanish Citizens' Security Bill: Many restrictions, few freedoms*, 28th January 2015, available at https://edri.org/spanish-citizens-security-bill-many-restrictions-few-freedoms/

Fernández Pérez, M., *Spanish Citizens' Security law: There is still some hope*, 8th April 2015, available at https://edri.org/spanish-citizens-security-law-hope-not-lost/

Fiedler, K., *EU Commission set to re-brand the failed CleanIT project*, 3rd June 2015, available at https://edri.org/eu-commission-rebrand-failed-cleanit-project/

Fiedler, K., *Patriot Act à la française: Braucht Frankreich weitere Überwachungsmaßnahmen?*, 26th January 2015, available at https://netzpolitik.org/2015/franzoesischer-patriot-act-ueberwachungsmassnahmen/
Free Speech Debate, *Article 19: freedom of expression anchored in international law*, 10th February 2012, available at http://freespeechdebate.com/en/discuss/article-19-freedom-of-expression-anchored-in-international-law/

Fullerton, J., *This App Lets China's Netizens Use Twitter Where It's Censored*, 9th June 2015, available at http://motherboard.vice.com/read/this-app-lets-chinas-netizens-use-twitter-where-its-censored

Global Voices, *China Gives Internet Celebrities a Guide for Self-Censorship*, 13th August 2013, available at http://globalvoicesonline.org/2013/08/13/china-creates-guideline-for-Internet-celebrities-self-censorship/

Global Voices Advocacy, *China: Over 100,000 Weibo Users Punished for Violating 'Censorship Guidelines'*, 13th November 2013, available at http://advocacy.globalvoicesonline.org/2013/11/13/china-over-100000-weibo-users-punished-for-violating-censorship-guidelines/

Global Voices Advocacy, *Human Rights Verdict Could Affect Cisco in China,* 24th April 2013, available at http://advocacy.globalvoicesonline.org/2013/04/24/human-rights-verdict-could-affect-cisco-in-china/

Guilford, G., *LinkedIn is censoring posts about Tiananmen Square*, 4th June 2014, available at http://qz.com/216691/linkedin-is-censoring-posts-about-tiananmen-square-even-outside-mainland-china/

IGFWatch news, *Debunking eight myths about multi-stakeholderism*, 25th April 2015, available at http://igfwatch.org/discussion-board/debunking-eight-myths-about-multi-stakeholderism

Kleinwächter, W., *Internet Governance Outlook 2015: Two Processes, Many Venues, Four Baskets*, 3rd January 2015, available at http://www.circleid.com/posts/20150103_internet_governance_outlook_2015_2_processes_many_venues_4_baskets/

Kulicova, A., *China-Russia cyber-security pact: Should the US be concerned?,* Russia Direct, 21st May 2015, available at http://www.russia-direct.org/analysis/china-russia-cyber-security-pact-should-us-be-concerned

L'OBS*, Cinq sites "faisant l'apologie du terrorisme" bloqués pour la première fois en France*, 16th March 2015, available at http://tempsreel.nouvelobs.com/societe/20150316.AFP1833/cinq-sites-internet-bloques-pour-apologie-du-terrorisme-une-premiere-en-france.html

La Quadrature du Net, *Loi Cazeneuve : bientôt tous présumés terroristes ?*, 21st July 2014, available at http://www.laquadrature.net/fr/loi-cazeneuve-bientot-tous-presumes-terroristes

La Quadrature du Net, *Publication d'un mémoire citoyen au Conseil Constitutionnel contre la loi Renseignement !*, 23rd June 2015, available at http://www.laquadrature.net/fr/publication-dun-memoire-citoyen-au-conseil-constitutionnel-contre-la-loi-renseignement

Libertus, *Web sites: U.K. Internet Watch Foundation ("IWF") 2008 & 2007 statistics, in* Statistics Laundering: false and fantastic figures, 2009, available at http://libertus.net/censor/resources/statistics-laundering.html#iwfstats

Matheny, S., *Net Neutrality: The Struggle for Internet Freedom*, 30th September 2013, available at http://globalsolutions.org/blog/2013/09/Net-Neutrality-Struggle-Internet-Freedom#.VYaIjUa1dcM

MacKinnon, R., *Global Online Freedom Act is re-introduced*, 11th January 2007, available at http://rconversation.blogs.com/rconversation/2007/01/global_online_f.html

Marks, K., *The BPI's China-like clauses in the Digital Economy Bill*, 23rd March 2010, available at http://epeus.blogspot.be/2010/03/bpis-china-like-clauses-in-digital.html

Masnick, M., *Are People In China Happy With The Great Firewall?,* 16th May 2008, https://www.techdirt.com/articles/20080515/0258451120.shtml

Masnick, M., *China Gleefully Uses UK Desire For Censorship To Validate Its Own Censorship,* 12th April 2011, available at https://www.techdirt.com/articles/20110812/10553415491/china-gleefully-uses-uk-desire-censorship-to-validate-its-own-censorship.shtml

Masnick, M., *China: Great Firewall isn't censorship, it's safeguarding the public*, 21st October 2011, available at https://www.techdirt.com/articles/20111020/03291216428/china-great-firewall-isnt-censorship-its-safeguarding-public.shtml

Masnick, M., *China Learned The Tricks of Propaganda From The Best: US Politicians & PR Industry,* 5th June 2014, https://www.techdirt.com/articles/20140604/12125327461/china-learned-tricks-propaganda-best-us-politicians-pr-industry.shtml

Masnick, M., *Chinese Lessons For SOPA/PIPA: The Great Firewall Of China Was Once A Way To Stop Infringement Too*, 23rd January 2012, available at https://www.techdirt.com/articles/20120119/17271917481/chinese-lessons-sopapipa-great-firewall-china-was-once-way-to-stop-infringement-too.shtml

Masnick, M., *DNS Screwup Accidentally Extends Great Firewall Of China To Chile And The US?,*26th March 2010, available at https://www.techdirt.com/articles/20100326/2241128746.shtml

Masnick, M., *EU Parliament Wants China To Join ACTA, Even As It May Reject It?,* 25th May 2012, available at https://www.techdirt.com/articles/20120524/03204119058/eu-parliament-wants-china-to-join-acta-even-as-it-may-reject-it.shtml

Masnick, M., *Father Of The Great Firewall Defends Chinese Internet Censorship By Noting The US Does The Same Thing*, available at https://www.techdirt.com/articles/20110218/01583213162/father-great-firewall-defends-chinese-Internet-censorship-noting-us-does-same-thing.shtml

MacKinnon, R., *Google and Internet Control in China. Congressional-Executive Commission on China*, 24th March 2010, available at http://rconversation.blogs.com/MacKinnonCECC_Mar24.pdf

Masnick, M., *Is the Great Firewall of China a Trade Barrier? And If So, Does China Care?*, 17th May 2010, available at https://www.techdirt.com/articles/20100517/0102209437.shtml

Masnick, M., *Tell The UN To Keep Its Hands Off The People's Internet,* 1st June 2012, available at https://www.techdirt.com/articles/20120601/10182719172/tell-un-to-keep-its-hands-off-peoples-Internet.shtml

Masnick, M., *That's Rich: China Accuses Google Of Censorship*, 28th October 2009, available at https://www.techdirt.com/articles/20091027/1754316700.shtml

Masnick, M., *The Similarity Between ACTA And Chinese Internet Censorship*, 20th January 2010, available at https://www.techdirt.com/articles/20100120/0216537828.shtml

Masnick, M., *Will Google Pull Out Of India, Australia And Other Countries Over Internet Censorship?,* 14th January 2010, available at https://www.techdirt.com/articles/20100113/2252047738.shtml

McNamee, J., *EU and China adopt harmonised approach to censorship*, 18th May 2011, available at http://edri.org/edrigramnumber9-10eu-china-censorship-Internet/

McNamee, J., *Google's right to be forgotten – industrial scale of misinformation*, 19th June 2014, available at http://edri.org/forgotten/

McNamee, J., *NETmundial, multistakeholderism and fair process*, 7th May 2014, available at http://edri.org/enditorial-netmundial-multistakeholderism-and-fair-process/

McNamee, J., *Privatised online enforcement series: A. Abandonment of the rule of law*, 23rd March 2011, available at https://edri.org/edrigramnumber9-6abandonment-rule-of-law/

Moody, G., *Russia And China Both Want To 'Protect Children'; Both Want To Do It By Increasing Censorship*, 13th July 2012, available at https://www.techdirt.com/articles/20120712/07000519673/russia-china-both-want-to-protect-children-both-want-to-do-it-increasing-censorship.shtml

Muller, M., *NetMundial moves net governance beyond WSIS*, 27th April 2014, available at http://www.Internetgovernance.org/2014/04/27/netmundial-moves-net-governance-beyond-wsis/

Musiani, F. and Pohle, J., *NETmundial: only a landmark event if 'Digital Cold War' rhetoric abandoned*, 27th March 2014, available at http://policyreview.info/articles/analysis/netmundial-only-landmark-event-if-digital-cold-war-rhetoric-abandoned

Olukotun, D., *Human Rights Verdict Could Affect Cisco in China*, 24th April 2013, available at http://advocacy.globalvoicesonline.org/2013/04/24/human-rights-verdict-could-affect-cisco-in-china/

Open Rights Group, *ORG's Blocked project finds almost 1 in 5 sites are blocked by filters*, available at https://www.openrightsgroup.org/press/releases/orgs-blocked-project-finds-almost-1-in-5-sites-are-blocked-by-filters

Reporteurs Sans Frontières, *La liberté d'information menacée au nom de l'urgence terroriste*, 18th July 2014, available at http://fr.rsf.org/france-la-liberte-d-information-menacee-18-07-2014,46659.html

Sloan, A., *China ramps up army of "opinion monitors"*, 25th March 2014, available at http://www.indexoncensorship.org/2014/03/china-opinion-monitors/

Talib, C., *France adopts anti-terror law eroding civil liberties*, 24th September 2014, available at https://edri.org/france-adopts-anti-terror-law/

The Privacy Surgeon (Davies, S., Ed.), *A Crisis of Accountability. A global analysis of the impact of the Snowden revelations*, June 2014, available at http://www.privacysurgeon.org/blog/wp-content/uploads/2014/06/Snowden-final-report-for-publication.pdf

Books

Belli, L. and De Filippi, P. (Eds.), The Value of Network Neutrality for the Internet of Tomorrow, Report of the Dynamic Coalition on Network Neutrality, November 2013.

Ginsburg, *Law and the Liberal Transformation of the Northeast Asian Legal Complex in Korea and Taiwan,* Fighting for Political Freedom: Comparative Studies of the Legal Complex and Political Change, Oxford: Hart Press, 2007

Hogge, B., A Guide to the Internet for Human Rights Defenders, Barefoot Publishing Limited, 2014

Jakubowicz, K., *Media revolution in Europe: ahead of the curve*, Council of Europe Publishing, August 2011

Lamarca Pérez, C. et al, Derecho Penal. Parte especial, Ed. Colex, 4th Edition, Madrid, 2008

Landau, S., Surveillance or Security? The Risks Posed by New Wiretapping Technologies, Massachusetts Institute of Technology, 2010

Li, Y., The Judicial System and Reform in Post-Mao China: Stumbling Towards Justice, The rule of law in China and Comparative Perspectives, Ed. Ashgate Publishing Limited, England, 2014

Mattei, U. and Nader, L., Plunder. When the Rule of Law is Illegal, Blackwell Publishing, United Kingdom, 2008

Noya, J. (dir.) and others, La imagen de España en China, Real Instituto Elcano de Estudios Internacionales y Estratégicos, January 2007

Peña González, J., Derecho y Constitución, Ed. Dykinson S.L., Madrid, 2004

Shapiro, A., The Control Revolution: How the Internet is Putting Individuals in Charge and Changing the World. Public Affairs, New York, 1999

Simitis,S., Reviewing Privacy in an Information Society, 135 U.PA. L. REV. 707, 734, 1987

Tai, Z., The Internet in China: Cyberspace and Civil Society, Ed. Routledge, New York, 2006

Thierer, A. and Crews, C.W. (Eds.), Who rules the net? Internet governance and jurisdiction, Washington D.C., The Cato Institute, 2003

Yong, H., Spreading the news, in Schmidt, N. (Ed.), *Digital Frontiers*, Index on censorship, Volume 21. No. 4, Sage Publications, 2012

Case law

Constitutional Court of Chile, Court ruling of 12th July 2011, available at http://www.tribunalconstitucional.cl/wp/ver.php?id=2011

Court of Justice of the European Union, *UPC Telekabel Wien GmbH v. Constantin Film Verleih GmbH, Wega Filmproduktionsgesellschaft mbH*, C-314/12, 27th March 2014, available at http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:62012CJ0314&from=EN

District court for the District of Maryland, *Du Daobin, et al. v. Cisco Systems, Inc. et al.,* case 8:11-cv-01538-PJM, 24th February 2014, available at https://www.eff.org/files/2014/02/24/4995755-0-12686.pdf

ECtHR, *Delfi AS v. Estonia*, Application no. 64569/09, 10th October 2013, available at http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-126635#{%22itemid%22:[%22001-126635%22]}

ECtHR, *Delfi AS v. Estonia*, Application No. 64569/09, Grand Chamber, 16th June 2015, available at http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-155105#{%22itemid%22:[%22001-155105%22]}

ECtHR, *Silver and others v. UK*, no.5947/72; 6205/73; 7052/75; 7061/75; 7107/75; 7113/75; 7136/75; Kudla v. Poland, no. 30210/96.

French Constitutional Court, ruling No. 2015-713 DC of 23rd July 2015, available at http://www.conseil-constitutionnel.fr/conseil-constitutionnel/francais/les-decisions/acces-par-date/decisions-depuis-1959/2015/2015-713-dc/decision-n-2015-713-dc-du-23-juillet-2015.144138.html (last visited on 4th August 2015).

Supreme Court of Estonia, *Vjatšeslav Leedo v. AS Delfi*, 3-2-1-43-09, 10th June 2009.

Legislation

Central Committee of the Chinese Communist Party, Decision to "accelerate the construction of a Socialist rule of law country", 28th October 2014, available in English at https://chinacopyrightandmedia.wordpress.com/2014/10/28/ccp-central-committee-decision-concerning-some-major-questions-in-comprehensively-moving-governing-the-country-according-to-the-law-forward/

Charter of Fundamental Rights of the European Union, available at http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:12010P&from=EN

China Copyright and Media, China's State Internet Information Office: Regulation on the Management of Internet User Accounts, 4th February 2015, available at https://chinacopyrightandmedia.wordpress.com/2015/02/04/internet-user-account-name-management-regulations/; Chinese version available at http://www.cac.gov.cn/2015-02/04/c_1114246561.htm

Chinese Computer Information Network and Internet Security, Protection and Management Regulations, 30th December 1997, available at http://fas.org/irp/world/china/netreg.htm

Chinese Constitution

Chinese Civil Procedure Law, 2007

Chinese Criminal Law, 1997

"Code de procédure pénale français", available at http://www.legifrance.gouv.fr/affichCode.do;jsessionid=56FC6E2ACAD19750B5D2F073F07E3AC0.tpdila16v_3?cidTexte=LEGITEXT000006071154&dateTexte=20150804

"Code des postes et des communications électroniques français", available at http://www.legifrance.gouv.fr/affichCode.do?cidTexte=LEGITEXT000006070987

Décret [français] n° 2009-86 du 22 janvier 2009 modifiant le décret n° 96-926 du 17 octobre 1996 relatif à la vidéosurveillance, available at http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000020146614&dateTexte=&categorieLien=idblank

Décret [français] n° 2015-253 du 4 mars 2015 relatif au déréférencement des sites provoquant à des actes de terrorisme ou en faisant l'apologie et des sites diffusant des images et représentations de mineurs à caractère pornographique, available at http://legifrance.gouv.fr/affichTexte.do;jsessionid=?cidTexte=JORFTEXT000030313562&dateTexte=&oldAction=dernierJO&categorieLien=id

Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market, available at http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32000L0031&from=EN

Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector, available at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0058:en:HTML

European Commission, Proposal for a Regulation of the European Parliament and of the Council laying down measures concerning the European single market for electronic communications and to achieve a Connected Continent, and amending Directives 2002/20/EC, 2002/21/EC, 2002/22/EC, and Regulations (EC) No 1211/2009 and (EU) No 531/2012 - COM(2013) 627 final, 11th September 2013, available at http://ec.europa.eu/digital-agenda/en/connected-continent-single-telecom-market-growth-jobs

European Commission, European Parliament and Council of the European Union, Interinstitutional Agreement on better law making, 2003, available at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2003:321:0001:0005:EN:PDF

European Parliament, Legislative powers. Ordinary legislative powers, available at http://www.europarl.europa.eu/aboutparliament/en/20150201PVL00004/Legislative-powers

European Parliament legislative resolution of 3rd April 2014 on the proposal for a regulation of the European Parliament and of the Council laying down measures concerning the European single market for electronic communications and to achieve a Connected Continent, and amending Directives 2002/20/EC, 2002/21/EC, 2002/22/EC, and Regulations (EC) No 1211/2009 and (EU) No 531/2012 (COM(2013)0627 – C7-0267/2013 – 2013/0309(COD)), available at http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P7-TA-2014-0281+0+DOC+XML+V0//EN

US Cybersecurity Information Sharing Act of 2015, S.754 , 114th Congress (2015-2016), available at https://www.congress.gov/bill/114th-congress/senate-bill/754

US Global Online Freedom Act of 2013, available at http://beta.congress.gov/bill/113th-congress/house-bill/491

Government of the Russian Federation, Order No. 788-p on signing the Agreement between the Government of the Russian Federation and the Government of the People's Republic of China regarding International CyberSecurity, 30th April 2015, available at http://government.ru/media/files/5AMAccs7mSlXgbff1Ua785WwMWcABDJw.pdf

Judges Law of the People's Republic of China, 2001.

Law of the People's Republic of China on the Protection of Minors, 26th October 2012, available at http://www.lawinfochina.com/display.aspx?id=12626&lib=law&SearchKeyword=protection%20minors&SearchCKeyword=

Ley Federal de Telecomunicaciones y radiodifusión, Mexico, 14 July 2014, available at http://www.diputados.gob.mx/LeyesBiblio/ref/lftr/LFTR_orig_14jul14.pdf

Ley Orgánica 4/2015, de 30 de marzo, de protección de la seguridad ciudadana, Spain, available at http://www.boe.es/diario_boe/txt.php?id=BOE-A-2015-3442

Loi [française] n° 2001-1062 du 15 novembre 2001 relative à la sécurité quotidienne, available at http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000222052&dateTexte=&categorieLien=id

Loi [française] n° 2002-1094 du 29 août 2002 d'orientation et de programmation pour la sécurité intérieure, available at http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000780288

Loi [française] n° 2003-239 du 18 mars 2003 pour la sécurité intérieure, available at http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=LEGITEXT000005634107&dateTexte=vig

Loi [française] n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique, available at http://legifrance.gouv.fr/affichTexte.do;jsessionid=2509631E5AE8978FD31614987761D29B.tpdila23v_1?cidTexte=JORFTEXT000000801164&dateTexte=20150629

Loi [française] n° 2006-64 du 23 janvier 2006 relative à la lutte contre le terrorisme et portant dispositions diverses relatives à la sécurité et aux contrôles frontaliers, available athttp://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000454124&dateTexte=&categorieLien=id

Loi [française] n° 2011-267 du 14 mars 2011 d'orientation et de programmation pour la performance de la sécurité intérieure (LOPSI II), available at http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000023707312&dateTexte=&categorieLien=id

Loi [française] n° 2014-1353 du 13 novembre 2014 renforçant les dispositions relatives à la lutte contre le terrorisme, available at http://www.legifrance.gouv.fr/affichTexte.do;jsessionid=734BDF263C832C9D3D0CD91191F5F5C8.tpdila24v_2?cidTexte=JORFTEXT000029754374&dateTexte=29990101

Organic Law of the People's courts of the People's Republic of China

Projet de loi relatif au renseignement, Legislative dossier, France, available at http://www.assemblee-nationale.fr/14/dossiers/renseignement.asp

Miscellaneous

Barzun, M. W., speech given at the 2014 International IP Enforcement Summit in London, 12th June 2014, available at https://sslrelay.com/switchnewmedia.com/internationalipenforcementsummit/VOD/Matthew_W_Barzun_Video_Archive.php

Business & Human Rights Resource Centre, available at http://business-humanrights.org/en/un-secretary-generals-special-representative-on-business-human-rights

Cazeneuve, B. (coord.), Joint statement, Paris, 11th January 2015, available at https://www.bmi.bund.de/SharedDocs/Downloads/DE/Kurzmeldungen/gemeinsame-erklaerung.pdf?__blob=publicationFile

IANA, *Number resources*, available at https://www.iana.org/numbers

ICANN, Infographic, *Who Runs the Internet?*, 2013, available at www.xplanations.com/whorunstheinternet

ITU, *Basic Information - Frequently asked questions*, available at http://www.itu.int/wsis/basic/faqs.asp

ITU, *Membership*, available at https://www.itu.int/en/about/Pages/membership.aspx

Kaye, D., Statement to the 69th session of the UN General Assembly, 23rd October 2014, New York, available at http://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=15220&LangID=E

Microsoft, Code of conduct, updated in April 2009, available at http://windows.microsoft.com/en-us/windows-live/code-of-conduct

http://www.alexa.com

http://beta.congress.gov/bill/113th-congress/house-bill/491

https://www.blocked.org.uk

http://www.bostoncommonasset.com/news/Investor-Statement-ATS-FINAL.pdf

http://www.china.org.cn/english/Political/29034.htm

http://www.computerhope.com/issues/ch001016.htm

http://content.netmundial.br/contribution/international-code-of-conduct-for-information-security/67

https://en.greatfire.org/

https://en.rsf.org/

http://europa.eu/about-eu/institutions-bodies/

http://guides.library.harvard.edu/chineselegalresearch

https://globalnetworkinitiative.org/faq/index.php

https://globalnetworkinitiative.org/participants/index.php

http://www.greatfirewallofchina.org/

http://www.howtogeek.com/161808/htg-explains-what-is-dns-cache-poisoning/

http://www.hrw.org/get-involved

https://www.iana.org

http://icannwiki.com/index.php/Internet_Society

http://www.igovernment.in/igov/editorial/39494/consensus-netmundial

http://www.Internetgovernance.org/wordpress/wp-content/uploads/2014-03-ICANN-IANA-Role-Structures.pdf

http://www.itu.int/itudoc/gs/promo/gs/member/80531.pdf

http://www.itu.int/en/wcit-12/Pages/default.aspx

http://www.itu.int/wsis/basic/faqs.asp

http://justnetcoalition.org

http://mediafreedom.ushahidi.com/

https://www.netmundial.org/about

http://netmundial.br/wp-content/uploads/2014/04/NETmundial-Multistakeholder-Document.pdf

http://www.netneutrality.in/

https://www.nsa-observer.net/

http://www.olemiss.edu/courses/pol324/chnjudic.htm

http://www.osce.org/fom/118298

http://www.osce.org/fom/118298?download=true

http://www.pen.org/defending-writers/test-first-name-test-middle-name-test-last-name/yang-tongyan

https://presumes-terroristes.fr/

https://snowdenarchive.cjfe.org/greenstone/cgi-bin/library.cgi

http://www.talktalk.co.uk/security/homesafe-demo.html

http://www.huawei.com/ilink/en/success-story/HW_196215

http://www.transparency.org/country#CH

http://www.transparency-initiative.org/about/definitions

https://www.wepromise.eu/en/page/charter

Official reports

Latvian Presidency of the Council of the European Union, *Proposal for a Regulation of the European Parliament and of the Council laying down measures concerning the European single market for electronic communications and to achieve a Connected Continent, and amending Directives 2002/20/EC, 2002/21/EC and 2002/22/EC and*

Regulations (EC) No 1211/2009 and (EU) No 531/2012 - Examination of the Presidency compromise text on net neutrality, 1 3555/13 TELECOM 232 COMPET 646 MI 753 CONSOM 161 CODEC 2000, 20th January 2015, p.3, available at http://data.consilium.europa.eu/doc/document/ST-5439-2015-INIT/en/pdf

Bilbao-Osorio, B., Dutta, S. and Lanvin, B. (Edrs.), *The Global Information Technology Report 2014 Rewards and Risks of Big Data*, Insight Report - World Economic Forum and INSEAD, 2014, available at http://www3.weforum.org/docs/WEF_GlobalInformationTechnology_Report_2014.pdf

CCA Advogados, *Legal Guide for Foreign Investors in China*, 20th September 2010, available at http://www.cca-advogados.com/xms/files/Guia_Resumido_ING_02_reduzido.pdf

Comité d'Experts sur le terrorisme, *Profils nationaux relatifs à la capacité de lutte contre le terrorisme: France*, Council of Europe, September 2013, available at http://www.coe.int/t/dlapil/codexter/Country%20Profiles/Profiles%202013%20France_FR.pdf

Commissioner for Human Rights, *The rule of law on the Internet and in the wider digital world, Issue Paper*, CommDH/IssuePaper(2014)1 prepared by Prof. Douwe Korff, Council of Europe, 8th December 2014, available at https://wcd.coe.int/com.instranet.InstraServlet?command=com.instranet.CmdBlobGet&InstranetImage=2734552&SecMode=1&DocId=2262340&Usage=2

Commissioner for Human Rights, *Positions on counter-terrorism and human rights protection*, CommDH/PositionPaper(2015)1, Council of Europe, available at https://wcd.coe.int/com.instranet.InstraServlet?command=com.instranet.CmdBlobGet&InstranetImage=2757196&SecMode=1&DocId=2274090&Usage=2

Council of Europe, *Internet Governance Strategy 2012-2015*, available at https://wcd.coe.int/ViewDoc.jsp?id=1919461

CSIL and PPMI, *Internet, digital agenda and economic development of European regions*, Directorate-General for Internal Policies, Policy Department B: Structural and Cohesion Policies, Study, Vol. I., for the European Parliament's Committee on Regional Development, PE 513.970, September 2013, available at http://www.europarl.europa.eu/studies

EESC, *Opinion on Self-regulation and co-regulation in the Community legislative framework*, INT/754, 22nd April 2015, available at http://www.eesc.europa.eu/?i=portal.en.int-opinions.32859

European Commission, *A Digital Single Market Strategy for Europe*, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, COM(2015) 192 final, Brussels, 6th May 2015, available at http://ec.europa.eu/priorities/digital-single-market/docs/dsm-communication_en.pdf

European Commission, *Action Plan "Simplifying and improving the regulatory environment",* Communication from the Commission, COM(2002) 278 final - Not published in the Official Journal, 5th June 2002, available at http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=URISERV:l10108&from=EN

European Commission, *EU Charter of Fundamental Rights*, DG Justice, available at http://ec.europa.eu/justice/fundamental-rights/charter/index_en.htm

European Commission, *Scoreboard 2014 - Progress Report Digital Agenda Targets 2014*, 28th May 2014, available at https://ec.europa.eu/digital-agenda/en/news/scoreboard-2014-progress-report-digital-agenda-targets-2014

European Commission, *The European Agenda on Security*, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, COM(2015) 185 final, Strasbourg, 28th April 2015, available at http://ec.europa.eu/dgs/home-affairs/e-library/documents/basic-documents/docs/eu_agenda_on_security_en.pdf

European Commission, *The Internet Policy and Governance Europe's role in shaping the future of Internet Governance*, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, COM/2014/072 final, 12th February 2014, available athttp://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52014DC0072&from=EN

European Parliament (rapporteur Dati, R.,), Draft report *on prevention of radicalisation and recruitment of European citizens by terrorist organisations*, 2015/2063(INI), Committee on Civil Liberties, Justice and Home Affairs, 1st June 2015, available at http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-%2f%2fEP%2f%2fNONSGML%2bCOMPARL%2bPE-551.967%2b01%2bDOC%2bPDF%2bV0%2f%2fEN

European Parliament *Resolution on internet governance: the next steps*, (2009/2229(INI)), 15th June 2010, available at http://www.europarl.europa.eu/sides/getDoc.do?type=TA&reference=P7-TA-2010-0208&language=EN

European Parliament, *Resolution on the renewal of the mandate of the Internet Governance Forum*, 2015/2526(RSP), 11th February 2015, available at http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P8-TA-2015-0033+0+DOC+XML+V0//EN&language=GA

Google, *Transparency report*, available at http://www.google.com/transparencyreport/?hl=en-GB

Google, *Transparency Report on Traffic*, 2015, available at http://www.google.com/transparencyreport/traffic/disruptions/#region=CN&expand=Y2015

Human Rights Committee, General comment No. 34, Article 19: Freedoms of opinion and expression,102nd session, July 2011, U.N. Doc. CCPR/C/GC/34.

Human Rights Council, Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue, U.N. Doc. A/HRC/23/40

IMCO, *Hearing of Andrus Ansip, Vice-President and Commissioner-Designate (Digital Single Market)*, available at http://www.elections2014.eu/resources/library/media/20141022RES75838/20141022RES75838.pdf

Information Office of the State Council of the People's Republic of China, *White Paper on the Internet in China*, Beijing, 8 June 2010, available at http://www.china.org.cn/government/whitepaper/node_7093508.htm

Internet Society, *Understanding the WSIS+10 Review Process, The UN and its 10-year Review of the WSIS in December 2015*, May 2015, available at https://www.internetsociety.org/sites/default/files/WSISplus10-Overview.pdf

Intelligence and Security Committee, *Foreign involvement in the Critical National Infrastructure. The implications for national security,* June 2013, available at https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/205680/ISC-Report-Foreign-Investment-in-the-Critical-National-Infrastructure.pdf

ITU, *Measuring the Information Society Report 2014*, 24th November 2014, available at http://www.itu.int/en/ITU-D/Statistics/Documents/publications/mis2014/MIS2014_without_Annex_4.pdf

ITU, *Resolution 73 of the ITU Plenipotentiary Conference*, Minneapolis, 1998, available at http://www.itu.int/wsis/docs/background/resolutions/73.html

MacDonald, R., Ben-Avie, J. and Carrion, F., Internet freedom and the right to private life, protection of personal data and due process of law, Report drafted by Access for the Council of Europe, MCM(2013)008, 2013

McNamee, J., *The Slide From "Self-Regulation" to corporate censorship*, EDRi booklet, 25th September 2011, available at https://edri.org/wp-content/uploads/2010/01/selfregualation_paper_20110925_web.pdf

McNamee, J. and Fernández Pérez, M. (Eds.), Human Rights Violations Online, drafted by European Digital Rights for the Council of Europe, DGI(2014)31, 4th December 2014, available at https://edri.org/files/EDRI_CoE.pdf

Media Consulting Group, *The Potential for Cultural Exchanges between the European Union and Third Countries: The Case of China*, Study, European Parliament, DG for Internal policies, Policy Department B: structural and cohesion policies, April 2009, available at http://www.europarl.europa.eu/RegData/etudes/etudes/join/2009/419097/IPOL-CULT_ET%282009%29419097_EN.pdf

Microsoft, *Cyberspace 2025: Today's Decisions, Tomorrow's Terrain*, June 2014, available at http://www.google.be/url?sa=t&rct=j&q=&esrc=s&source=web&cd=2&ved=0CCUQFjAB&url=http%3A%2F%2Fdownload.microsoft.com%2Fdownload%2FC%2F7%2F7%2FC7775937-748E-4E95-85FB-24581F16B588%2FCyberspace%25202025%2520Today%25E2%2580%2599s%2520Decisions%2C%2520Tomorrow%25E2%2580%2599s%2520Terrain.pdf&ei=T8SjU_-dKYW4O6CtgdAG&usg=AFQjCNH1bX4VsVzi0V9j62J2XrzdHzn78A&bvm=bv.69411363,d.ZWU

Ministry of Foreign Affairs of the People's Republic of China, *China Reacts Strongly to US Announcement of Indictment Against Chinese Personnel,* 19th May 2014, available at http://www.fmprc.gov.cn/mfa_eng/xwfw_665399/s2510_665401/2535_665405/t1157487.shtml

The National People's Congress of the People's Republic of China, *China adopts national security law*, Press release, Beijing, 1st July 2015, available at http://www.npc.gov.cn/englishnpc/news/Legislation/2015-07/01/content_1940329.htm (last visited on 5th August 2015).

The National People's Congress of the People's Republic of China, *China Seeks public views on new cyber security law*, Press release, Beijing, 8th July 2015, available at http://www.npc.gov.cn/englishnpc/news/2015-07/10/content_1941413.htm

NIC, *Global Trends 2030: Alternative worlds*, US National Intelligence Council, available at http://globaltrends2030.files.wordpress.com/2012/11/global-trends-2030-november2012.pdf

OECD, *China, Information Technologies and the Internet*, OECD Information Technology Outlook 2006, OECD Publishing, available at 10.1787/it_outlook-2006-6-enpp

OECD, *The Economic and Social Role of internet Intermediaries*, April 2010, available at http://www.oecd.org/internet/ieconomy/44949023.pdf

Office of the High Commissioner on Human Rights, State communication surveillance undermines freedom of expression, warns UN expert, 4th June 2013, available at: http://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=13400&LangID=E

OHCHR, *Vienna Declaration and Programme of Action*, 25th June 1993, para. 5, available at http://www.ohchr.org/EN/ProfessionalInterest/Pages/Vienna.aspx

Olivié, I., Gracia, M. and García-Calvo, C., *Informe Elcano de Presencia global*, Real Instituto Elcano, 23rd April 2014, available at http://www.globalpresence.realinstitutoelcano.org/es/data/Presencia_Global_2014.pdf

Recommendation CM/Rec(2014)6 of the Committee of Ministers to member States on a Guide to human rights for Internet users, 16th April 2014, available at https://wcd.coe.int/ViewDoc.jsp?id=2184807

Recommendation CM/Rec(2014)6 of the Committee of Ministers to member States on a guide to human rights for Internet users – Explanatory Memorandum, 16th April 2014, available at https://wcd.coe.int/ViewDoc.jsp?Ref=CM%282014%2931&Language=lanEnglish&Ver=addfinal&Site=CM&BackColorInternet=C3C3C3&BackColorIntranet=EDB021&BackColorLogged=F5D383

Rights International Spain and others, *Análisis de la Ley Orgánica 4/2015, de 30 de marzo, de Protección de la Seguridad Ciudadana a los efectos de la posible vulneración de los artículos 1, 9.2, 10.1, 14, 15, 20, 21, 24 y 25 de la Constitución Española*, available at http://rightsinternationalspain.org/uploads/publicacion/3d3d492cacc2a6705ccec427f61dd51b86c0f94b.pdf

Schwab, K. (Ed.) et al., *Global Competitiveness Report 2014-2015*, World Economic Forum, available at http://www3.weforum.org/docs/WEF_GlobalCompetitivenessReport_2014-15.pdf

UN Human Rights Council, *The promotion, protection and enjoyment of human rights on the Internet*, UN Doc. A/HRC/20/L.13, 5th July 2012

UN Secretary-General, *Report on the Rule of Law and Transitional Justice in Conflict and Post-Conflict Societies*, S /2004/616, 23rd August 2004, available at http://daccess-dds-ny.un.org/doc/UNDOC/GEN/N04/395/29/PDF/N0439529.pdf?OpenElement

UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Report, 16th May 2011, A/HRC/17/27, available at http://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf

Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion, 21st August 2014, available at https://www.crin.org/sites/default/files/freedomofexpression_2.pdf

UNESCO, *Fostering Freedom Online. The Role of Internet Intermediaries*, 19th January 2015, available at http://unesdoc.unesco.org/images/0023/002311/231162e.pdf

U.S. House of Representatives, *Investigative Report on the U.S. National Security Issues Posed by Chinese Telecommunications Companies Huawei and ZTE*, 8th October 2012, available at https://intelligence.house.gov/sites/intelligence.house.gov/files/documents/Huawei-ZTE%20Investigative%20Report%20(FINAL).pdf

WGIG, *Report of the Working Group on Internet Governance* (WGIG), June 2005, available at http://www.wgig.org/docs/WGIGREPORT.pdf

WSIS, *Geneva Declaration of Principles*, WSIS-03/GENEVA/DOC/0004, Geneva, 10th -12th December 2003, available at http://www.itu.int/dms_pub/itu-s/md/03/wsis/doc/S03-WSIS-DOC-0004!!PDF-E.pdf

WSIS, *Tunis Agenda for the Information Society*, WSIS-05/TUNIS/DOC/6(Rev. 1)-E, 18th November 2005, available at http://www.itu.int/wsis/docs2/tunis/off/6rev1.html

Zalnieriute, M. and Schneider, T., *ICANN's procedures and policies in the light of human rights, fundamental freedoms and democratic values*, Expert Report for the Council of Europe, DGI(2014)12, 16 June 2014, available at http://www.coe.int/t/dghl/standardsetting/dataprotection/TPD_documents/ICANN-PoliciesProcedures%2816June2014%29.pdf

Press

BBC News, *China tightens Internet controls,* 23rd February 2010, available at http://news.bbc.co.uk/2/hi/asia-pacific/8530378.stm

BBC News, *French government orders website block*, 26th March 2015, available at http://www.bbc.com/news/technology-31904542

Black, E., *China's Internet Censorship Harms Trade, US Companies*, 6th December 2011, available at http://www.forbes.com/sites/edblack/2011/12/06/chinas-Internet-censorship-harms-trade-us-companies/

Chen, G., Tsang, D. and Ren, D., *12 new free-trade zones to follow in Shanghai's footsteps*, South China Morning Post, 23rd January 2014, available at http://www.scmp.com/business/china-business/article/1411417/12-new-free-trade-zones-follow-shanghais-footsteps

China Daily, *China sets up State Internet information office*, 4th May 2011, available at http://www.chinadaily.com.cn/china/2011-05/04/content_12440782.htm

ComputerWire, *Cisco sues Huawei over IP 'theft'*, 24th January 2003, http://www.theregister.co.uk/2003/01/24/cisco_sues_huawei_over_ip/

DomainNewsAfrica, *A transition to decentralized Internet, but will we get there by 2015?,* 27th March 2014, available at http://domainnewsafrica.com/a-transition-to-decentralized-Internet-but-will-we-get-there-by-2015/

European Commission, *Inclusive governance for a global Internet*, press release (speech), 10th June 2014, available at http://europa.eu/rapid/press-release_SPEECH-14-447_en.htm

European Commission, Press Release - *La lutte contre le terrorisme au niveau européen: présentation des actions, mesures et initiatives de la Commission européenne*, 11th January 2015, available at http://europa.eu/rapid/press-release_MEMO-15-3140_fr.htm

European Commission, *Towards further Globalisation of the Internet*, Press release, 15th March 2014, available at http://europa.eu/rapid/press-release_STATEMENT-14-70_en.htm

ElMundo, *Las 44 conductas que se multan en la nueva 'ley mordaza'*, 1st July 2015, available at http://www.elmundo.es/espana/2015/07/01/559418d5268e3eb16d8b4582.html

Genachowski, J. and Goldstein, *G.M., 'Global' Internet Governance Invites Censorship*, 3rd April 2014, available at http://online.wsj.com/news/articles/SB10001424052702303978304579471670854356630

Gilbert, D., *Chinese anti-censorship group GreatFire.org hit by aggressive DDoS attack*, 23 March 2015, available at http://www.ibtimes.co.uk/chinese-anti-censorship-group-greatfire-org-hit-by-aggressive-ddos-attack-1493105

Global Times, *Web regulation in public's best interest*, 4th June 2013, http://www.globaltimes.cn/content/786493.shtml

Greenwald, G., *What's scarier: terrorism, or governments blocking websites in its name?*, The Intercept, 17th March 2015, available at https://firstlook.org/theintercept/2015/03/17/whats-scarier-terrorism-governments-unilaterally-blocking-websites-name/

Gouvernement Français, *#Antiterrorisme : Manuel Valls annonce des mesures exceptionnelles*, 21st January 2015, available at http://www.gouvernement.fr/antiterrorisme-manuel-valls-annonce-des-mesures-exceptionnelles

Hecker, M., *La menace terroriste en France*, Institut Français des Relations Internationales, 9th January 2015, interview available at http://www.ifri.org/fr/publications/editoriaux/actuelles-de-lifri/jihad-syrie-irak-un-defi-france

IGFWatch news, *Debunking eight myths about multi-stakeholderism*, 25th April 2015, available at http://igfwatch.org/discussion-board/debunking-eight-myths-about-multi-stakeholderism

Kroes, N., *My thoughts on NETmundial and the Future of Internet Governance*, available at http://ec.europa.eu/commission_2010-2014/kroes/en/content/my-thoughts-netmundial-and-future-internet-governance

MacKinnon, R., *Stop the Great Firewall of America*, 15th November 2011, available at http://www.nytimes.com/2011/11/16/opinion/firewall-law-could-infringe-on-free-speech.html?_r=0

Meyer, D., *EU's response to free speech killings? More internet censorship*, Gigaom, 11th January 2015, https://gigaom.com/2015/01/11/eu-response-to-free-speech-killings-more-internet-censorship/

New York Times, *Gmail is blocked in China after months of disruption*,30th December 2014, available at http://www.nytimes.com/2014/12/30/technology/gmail-is-blocked-in-china-after-months-of-disruption.html?hp&action=click&pgtype=Homepage&module=second-column-region&region=top-news&WT.nav=top-news&_r=1

New York Times, *Gregarious and direct China's web doorkeeper*, 2nd December 2014, available at http://www.nytimes.com/2014/12/02/world/asia/gregarious-and-direct-chinas-web-doorkeeper.html

NTIA, *NTIA Announces Intent to Transition Key Internet Domain Name Functions,* 14th March 2014, available at http://www.ntia.doc.gov/press-release/2014/ntia-announces-intent-transition-key-internet-domain-name-functions

Olmo, J.M., *La Ley de Seguridad obligará a identificarse con el DNI para usar locutorios y cibercafés*, 7th April 2014, available at http://www.elconfidencial.com/espana/2014-04-07/la-ley-de-seguridad-obligara-a-identificarse-con-el-dni-para-usar-locutorios-y-cibercafes_112647/

Reuters, *Insight: For Cisco and Huawei, a bruising rivalry reaches stalemate*, 22th November 2013, available at http://www.reuters.com/article/2013/11/22/us-cisco-huawei-insight-idUSBRE9AL0NO20131122

RTVE, *La oposición recurre ante el Tribunal Constitucional la ley de seguridad ciudadana*, 21st May 2015, available at http://www.rtve.es/noticias/20150521/oposicion-recurre-ante-tribunal-constitucional-ley-seguridad-ciudadana/1148155.shtml

South China Morning Post, *China to lift ban on Facebook – but only within Shanghai free-trade zone*, 24th September 2013, available at http://www.scmp.com/news/china/article/1316598/exclusive-china-lift-ban-facebook-only-within-shanghai-free-trade-zone?page=all

Spanish Minister of Interior, *Aprobado el Proyecto de Ley Orgánica de Protección de la Seguridad Ciudadana*, Press conference, available at http://www.interior.gob.es/web/interior/prensa/noticias/-/asset_publisher/GHU8Ap6ztgsg/content/id/2230243

The Guardian, *China tightens 'Great Firewall' Internet control with new technology*, 14th December 2012, available at http://www.theguardian.com/technology/2012/dec/14/china-tightens-great-firewall-Internet-control

The Guardian, *Edward Snowden: the whistleblower behind the NSA surveillance revelations*, available at http://www.theguardian.com/world/2013/jun/09/edward-snowden-nsa-whistleblower-surveillance

The Guardian, *Shi Tao: China frees journalist jailed over Yahoo emails*, 8th September 2013, available at http://www.theguardian.com/world/2013/sep/08/shi-tao-china-frees-yahoo

The Register, *That Snowden chap was SPOT ON says China*, available at http://www.theregister.co.uk/2014/05/28/that_snowden_chap_was_spot_on_says_china/ , 28th May 2014

Tibet Post International, *Tibet-related apps are censored by technology giant Apple*, 5th April 2013, available at http://www.thetibetpost.com/en/news/international/3309-tibet-related-apps-are-censored-by-technology-giant-apple

Tout l'Europe, *La liberté de la presse en Europe*, 15th January 2015, available at http://www.touteleurope.eu/actualite/la-liberte-de-la-presse-en-europe.html

UK Reuters, *U.S. vice president urges Chinese to challenge their leaders,* 4th December 2013, available at http://uk.reuters.com/article/2013/12/04/uk-china-usa-biden-idUKBRE9B30CX20131204

Statistics

Alexa, *Top Sites in China*, available at http://www.alexa.com/topsites/countries/CN

Alexa, *The top 500 sites on the web*, available at http://www.alexa.com/topsites

http://ajantriks.github.io/netmundial/contributions_org_type.html

http://ajantriks.github.io/netmundial/map_no_contrib_govt.html

http://ajantriks.github.io/netmundial/track_multistakeholder.html

China Internet Network Information Center, *Statistical Report on Internet Development in China*, January 2013, available at http://www1.cnnic.cn/IDR/ReportDownloads/201302/P020130312536825920279.pdf

Internet Live Stats, *Internet Users by Country*, July 2014, available at http://www.internetlivestats.com/internet-users-by-country/

The World Bank, *China,* available at http://data.worldbank.org/country/china