BUILDING A DEMOCRACY WITH 140 CHARACTERS: THE E-CITIZEN AND THE STATE A PROPOSAL FOR A REGULATORY FRAMEWORK TO GOVERN ONLINE DEMOCRATIC SPACES

RIM-SARAH ALOUANE

Référence de publication : Rim-Sarah Alouane. « Building a Democracy With 140 characters: The E-citizen And the State A Proposal For a Regulatory Framework To Govern Online Democratic Spaces". Communication présentée dans le cadre du IXe Congrès de l'Association International de Droit Constitutionnel à Oslo, 16-20 juin 2014.

BUILDING A DEMOCRACY WITH 140 CHARACTERS: THE E-CITIZEN AND THE STATE: A PROPOSAL FOR A REGULATORY FRAMEWORK TO GOVERN ONLINE DEMOCRATIC SPACES

Cyberspace may give freedom of speech more muscle than the First Amendment does. It may already have become literally impossible for a government to shut people up.
Mike Godwin.

INTRODUCTION

Whether or not people are ready, our future will be digital. The twenty-first century has heralded the Internet age and has brought empowering technologies to large segments of the global population, both in the North and South. Nowadays, it is almost impossible to avoid computers, smartphones or tablets, as well as social networks like Facebook and Twitter that play a key role in the development of digital democracy and civic expression.

Indeed, in this digital era, the citizen has become transnational, timeless and (hyper)active. Their voices rise and spread widely. Violations of civil rights and freedoms are now exposed on a global scale, and revolutions transcend borders and create global impact, as witnessed by the essential role social networks played in the Arab Spring.

However, digital technologies also present new challenges for democracy. New dematerialized risks are emerging, such as cybercrime or cyber surveillance. Even as the State slowly loses control of the online environment, it must still guarantee and ensure the protection of the e-citizen. These threats make necessary and urgent the creation and the establishment of new forms of regulation of the Internet to support, maintain and enhance the emergence of a genuine e-citizenship that can facilitate a more efficient and vigorous democracy.

This paper proposes a framework of regulation of the online democratic space that will ensure that the Internet can remain at the service of the expression of rights and freedoms, which are cornerstones of democracy.

1. The Fast Growth Of the E-Democracy: In Search Of An Efficient And Adapted Protection.

The rise of the Internet gave us the concept of digital community, and as those communities matured and sought ways to govern themselves, digital democracy was born. As the digital space grows, the web becomes a key element in the development of society (roles played by the telephone or television in another life), has deeply changed, and touched society. These innovations are disruptors that have major implications for communication in general, and individual freedoms, privacy and social relations in particular.

Democracy as we know it has been significantly affected by the landscape of new and social media. Vibrant new public gathering spaces in cyberspace emerged for each country as well as globally. This radical transformation of our democracy in only a few short years deserves to be analysed for the impact it has on society, governance, and the application of rights. As people shift their primary means of communication to online spaces, and begin to share their opinions, contribute to discussions, observe debates, and participate in political campaigns, individuals become e-citizens whose role in shaping societies is immensely more impactful.

But the development of the Web has not only brought positive aspects for democracy: indeed, it also brings up new risks that must be controlled and mitigated at some point. The same tools that make online voting, democracy education, and political participation possible also enable cybercrime and the increased monitoring of society. Further complicating matters, these otherwise negative impacts are also needed for the fight against terrorism and crime. It is therefore essential to create a balance that respects the rights of the emerging e-citizen, creates opportunities to safeguard society from real threats, and prevent security apparatuses from creating a global surveillance regime[1].

[1] Armand Mattelard, La globalisation de la surveillance: aux origines de l’ordre sécuritaire, La Découverte, Paris, 2007, 259 p.

Warren Chik, an Associate Professor of Law at Singapore Management University an authority on IT law, offers these helpful definitions:

> *"Computer Crime" encompasses crimes committed against the computer, the materials contained therein such as software and data, and its uses as a processing tool. These include hacking, denial of service attacks, unauthorized use of services and cyber vandalism. "Cyber Crime" describes criminal activities committed through the use of electronic communications media. One of the greatest concerns is with regard to cyber-fraud and identity theft through such methods as phishing, pharming, spoofing and through the abuse of online surveillance technology. There are also many other forms of criminal behaviour perpetrated through the use of information technology such as harassment, defamation, pornography, cyber terrorism, industrial espionage and some regulatory offences".*[2]

The rise of usage of computers and Internet due to the mass adoption of computer usage and connectivity[3] enabled a rapid development of online communities, and the pervasiveness of this community facilitates cybercrime on a global scale, including various violations of human rights and fundamental freedoms, and new delinquent or criminal behaviours emerge constantly. Examples of this evolution include child pornography, electronic commerce of illicit drugs, and websites that incite racial or religious hatred. A report written by the Japanese National Police Agency explains that:

> *"Cyberspace is being flooded with illegal and harmful information, and citizens are increasingly consulting the police on cases of online defamation and libel. With the emergence of previously unanticipated modus operandi and the extremely difficult situation of cybercrime investigation, and due to the high level of anonymity, many users have the distorted perception that "anything goes" in cyberspace, which could be reducing their respect for social norms*[4]*".*

Our aim is not to make a thorough analysis of cybercrime, but mainly to show that it has become a challenge for all countries, particularly for democracies, and to demonstrate that

[2] Warren B. Chik, 'Challenges to Criminal Law Making in the New Global Information Society: A Critical Comparative Study of the Adequacies of Computer-Related Criminal Legislation in the United States, the United Kingdom and Singapore' *in Cybercrime and the Law*, Icfai Law Books, 2007.

[3] Warren B. Chik, *Idem.*

[4] Japanese National Police Agency, *Report II : Creating a Safe, Responsible, Cybersociety* http://www.npa.go.jp/hakusyo/h23/english/PDF2.pdf (last accessed: 30 March 2014).

cyberspace should be given an adapted protection from such threats. Nevertheless, in order to do so, it is important to distinguish the different forms of action that can be classified as cybercrime.

Offenses can be broken down into several categories:
Offenses against the confidentiality and integrity of data and information systems.
Offenses against the interest of States.
Offenses related to the content of data.

Digital technologies are alternately objects of and resources for cybercrime. The *European Convention on Cybercrime* adopted in Budapest in 2001[5] aims to define the different types of cybercrime offenses in order to find a way to control and eradicate them.

In the beginning of the digital era, the initial concern concerned risks arising from the capacity of storage of data and hence, a potential violation of the rights and freedoms through the storage of personal data. France was one of the very first countries to enact a law that would regulate and control the developing of data storage and that would protect data privacy. The Law of 6 January 1978[6] states in its first article:

> *"Information technology should be at the service of every citizen. Its development shall take place in the context of international co-operation. It shall not violate human identity, human rights, privacy, or individual or public liberties".*

Given this law's very broad concept of the treatment of personal data, it easily adapted to the successive evolutions of technology thanks to the creation of the *National Commission on Informatics and Liberties* (*Commission Nationale de l'Informatique et des Libertés*), a French independent administrative authority7 body responsible for ensuring that information

[5] Convention on Cybercrime, 23 November 2001. http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm (last accessed: 30 March 2014).

[6] Law on Information, Technology, Data Files and Civil Liberties N° 78-17 of 6 January 1978 (*Loi Informatiques et Libertés*). Official translation: http://www.cnil.fr/fileadmin/documents/en/Act78-17VA.pdf (last accessed: 30 March 2014).

[7] For a further analysis on the notion of Independant Administrative Authority (*Autorité Administrative Indépendante*), see Laurence Calandri, *Recherche Sur la Notion de Régulation en Droit Administratif Français*, Librairie Générale de Droit et de Jurisprudence, 2009. 752 pp.

technology remains at the service of citizens and does not jeopardize human identity or breach human rights, privacy, or individual or public liberties[8].

As for trojans, spyware or viruses[9], they are considered as:

> *Essential tools a cybercriminal can use to obtain unauthorized access and steal information from a victim in an attack that usually constitutes the first phase. They settled without the knowledge of users and remain hidden while they download and install a more insidious threat*[10].

Other forms of damage to electronic systems include email bombings, which overload the email systems of a user so as to prevent it practical use, distributed denial of service (DDoS) attacks, which overwhelm a web server with false requests for service, and session hijacking, which interrupts the normal usage of a website with an alternate and possibly dangerous insertion of code. For example, the French law of 21 June 2004 on *Confidence in the Digital Economy* (*Loi Relative à la Confiance Numérique*[11]*)* penalized several of these malicious computer system behaviours. In normal operation, cookies can be safely used as a tool to store information on visitors in order to keep track of their activities on the Internet. However, they can also be used maliciously and therefore constitute a potential threat[12]. The use of encryption has been liberalized by French legislation passed on 26 July 1996 and 21 June 2004, and the most secure encryption protocols are no longer reserved only for Defence services. The use of such encryption, which is free but requires compliance with specific procedures, enables optimal protection of data privacy for public use.

2. Digital technologies as a tool for cybercrime.

[8] Further information: http://www.cnil.fr/english/the-cnil/ (last accessed: 30 March 2014)

[9] Further developments: Susan W. Brenner, Brian Carrier, and Jef Henninger, *The Trojan Horse Defense in Cybercrime Cases*, CERIAS Tech Report 2005-15. https://www.cerias.purdue.edu/assets/pdf/bibtex_archive/2005-15.pdf (last accessed: 30 March 2015).

[10] Myriam Quémener, Joël Ferry, *Cybercriminalité*, Economica, 2007 p 79. Our translation from French: *[Ils constituent des] outils essentiels qu'un cybercriminel peut utiliser pour obtenir des accès non autorisés et dérober des informations d'une victime dans le cadre d'une attaque dont ils constituent généralement la première phase. Ils s'installent à l'insu des utilisateurs et restent cachés tandis qu'ils téléchargent et installent une menace plus sournoise*.

[11] Law n°2004-575, 21 June 2004, Confidence in the Digital Economy (*Loi Relative à la Confiance Numérique)*.

[12] 'Internet Cookies Threaten Online Privacy', BBC News, 6 December 2011: http://www.bbc.co.uk/news/uk-northern-ireland-16042666 (last accessed: 30 March 2014).

According to Gabriel Weimann, a Professor of Communication at Haifa University and a cyberterrorism expert,

> *"The roots of the notion of cyberterrorism can be traced back to the early 1990s, when the rapid growth in Internet use and the debate on the emerging "information society*[13]*".*

Democracies must ensure that freedom of communication and exchange remain highly developed in the Internet age, are not side-tracked from their main purpose to promote other models far less respectful of rights and freedoms. Any proposal for a modern defence of online infrastructure from external threats must consider these new risks of destabilization. This assumes that democracies set up new forms of systems of protection adapted to these new risks, especially if such attacks are orchestrated by the State.

We are increasingly speaking of cyber warfare in addition to cyber terrorism. For example, during three weeks in in April and May of 2007, Estonia's online infrastructure suffered a severe attack[14] that caused the interruption and the blocking of the functioning of government institutions, public and private economic sectors, and the private use of computer networks by citizens. These attacks, which – according to Estonia – were encouraged, if not orchestrated, by Russia, are an example of the impact of cyber warfare and highlight the potential risks caused by this type of war. This concept of cyber warfare is not new, as the methods are inextricably linked to the development of computer networks. What is new, however, is its emergence as an independent form of conflict, and not just confined to standard information warfare.

The Internet has become a battle space within which cyber attacks are developed, and such attacks are increasingly difficult to attribute to any one State, even despite circumstantial evidence as is seen by the People's Army of China allegedly encouraging "patriotic hackers"

[13] Gabriel Weimann, 'Cyberterrorism : How Real is the Threat', *United States Institute Of Peace*, Special Report, p 2. http://www.usip.org/sites/default/files/sr119.pdf (last accessed: 30 March 2014).

[14] Further information: Jason Richards, 'Denial-of-Service: The Estonian Cyberwar and Its Implications for U.S. National Security' *International Affairs Review* : http://www.iar-gwu.org/node/65 (last accessed: 30 March 2014).

to conduct such attacks against foreign States. To fight and prevent these kinds of threats, NATO created a *Cyber Defense of Excellence in Estonia*[15] in 2008.

3. Digital technologies as a tool for cybersurveillance.

Neil Richards, a professor at the Washington University School of Law and a noted privacy expert, explains that:

> *"We are living in an age of surveillance. The same digital technologies that have revolutionized our daily lives over the past three decades have also created ever more detailed records about those lives"*[16].

The development of general insecurity in contemporary society, combined with the rise of terrorism and its climax with the attacks of 9/11 in the United States, led to the research and reinforcement of online security measures, sometimes to the detriment of individual freedoms. The balance between security and freedom should always be sought, even though it may be difficult to find. Armand Mattelart, a Belgian sociologist whose work deals with media, culture and communication, explains:

"Under democratic regimes, the multiplication of exceptions schemes under the 'global war' against terrorism, was combined since September 11, 2001 with the growing interference of monitoring daily lives of citizens... The climbing of military and police repression should not be forgotten that the tension between security and freedom, secrecy and transparency, coercion and consent, subjection and resistance is part of a long movement, less immediately visible"[17].

Online environments are susceptible to abuse by individuals and states that seek to use it as a highly efficient system of social control. Such abuse is made possible by manipulating the ever-increasing number of electronic footprints that each user leaves. E-citizens are increasingly comfortable with leaving electronic traces of their activity, and do not mind

[15] Further information: https://www.ccdcoe.org/ (last accessed: 30 March 2014).

[16] Neil M. Richards, 'The Dangers of Surveillance', 126 Harv. L. Rev. 1934 (2013), p 1936.

[17] Armand Mattelard, *op.cit.* Our translation from French: *« La multiplication des régimes d'exceptions dans le cadre de la 'guerre globale' contre le terrorisme, s'est conjugué depuis le 11 septembre 2001, sous les régimes démocratiques, avec l'ingérence croissante des dispositifs de surveillance dans la vie quotidienne des citoyens … L'escalade répressive, de nature à la fois militaire et policière, ne doit pas pour autant faire oublier que la tension entre sécurité et liberté, secret et transparence, contrainte et consentement, sujétion et résistance s'inscrit dans un mouvement long, moins immédiatement repérable* ».

transparency into their private lives. This leaves these communities susceptible to violations of their rights and privacy.

With all of their information readily available, it is easy to categorize online citizens in preparation for both benign uses (*e.g.* marketing) and abuse (*e.g.* identity theft). Anyone is easily identifiable according to various categories: student, employee, taxpayer, holder of a bank account, subscriber to a newspaper, trade unionist, political activist, and so on. The risk of hostile uses of these categories has increased, along with the potential for invasion of privacy and identity of those involved. Indeed, treatment of personal data is always created for a specific purpose that must be determined prior to its creation. In France, for example, this determination must be submitted to the CNIL with respect to a very specific process in order to prevent the hijacking of personal data from their initial purpose and to ensure the protection of a citizen's rights and freedoms.

E-government can also prove to be a very efficient system of social control, especially if some inoperability of information systems is possible. Thus, by visiting the websites of a particular government entity, Internet users leave traces that facilitate surveillance without even realizing it. Therefore, the risk of a generalized surveillance is real, even if it is not an intended purpose for that government entity. The absence of a sufficiently effective regulation and control can facilitate this unintended consequence. The risks of cyber surveillance are real because democracies seem to have changed this paradigm. Indeed, electronic traces left by web users have a great value for both private operators and public authorities. These traces are not only usable into the development of the digital economy but also for seeking information for reasons of national security. Neil Richards, a professor at Washington University in St. Louis and an expert in First Amendment and privacy law, underlines:

> *"We must recognize that surveillance transcends the public private divide. Public and private surveillance are simply related parts of the same problem, rather than being wholly discrete. Even if we are ultimately more concerned with government surveillance, any solution must grapple with the complex relationships between government and corporate watchers"*[18].

4. Censorship and surveillance behaviours.

[18] Neil M. Richards, *op.cit*. p.1935.

Digital censorship is implemented in many countries, for political or security reasons *(e.g* fight against terrorism) or to protect political regimes against opposition. For example, the fight against terrorism justified the adoption by the U.S. Congress on 25 October 2001 of a law symbolically called the USA PATRIOT Act[19]. This particular anti-terrorism law allows wiretapping of any communications device used by any person linked with a suspected terrorist. It makes it possible for the Federal Bureau of Investigation (FBI) to use monitoring software, such as the one named CARNIVORE, among Internet service providers to monitor the flow of email traffic and preserve Web histories of anyone suspected of being in contact with a foreign entity. This law covers a wide field, such as allowing recording, search and seizure of computers, stalking profile readers in libraries and other intrusive methods at the discretion of the Federal Police. Also, the FBI can issue security letters[20] without having to go through a judge to bankers, Internet access providers, telephone companies, credit agencies, travel agency, and libraries, requiring them to provide information about their customers. This Act has been met with substantial criticism, and its enactors have been accused of causing "an erosion of individual freedoms, private property rights, limited government and the rule of law[21]."

In 2007, the then-German Minister of Interior Wolfgang Schäuble requested authorization to get easier access to emails, on the grounds that "Informatics has become a parallel university and at the same time, a training camp for terrorists apprentices [22]". According to the Constitutional Court of Karlsruhe of 27 February 2008[23], computers owned by people who are suspected of committing a criminal offence may only be tapped using spying software but poses a limitation: this type of surveillance can only be done of this is necessary for the protection of extremely important general interests.

Authoritarian regimes do not hesitate to monitor users, and use whatever new technologies emerge. For example, the Iranian regime has set up a filter of websites they consider "immoral", such as those devoted to women's rights. In Burma, the government

[19] H.R.3162 -- Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001 (Enrolled Bill [Final as Passed Both House and Senate] - ENR)

[20] Maria Bustillos, 'How it Feels like to get a national security letter'? The NewYorker, 28 June 2013.

[21] Anne Rathbone & Charles K. Rowley, 'Terrorism', 111 Public Choice 9, 11 (2002).

[22] Daniel Vernet, 'La Justice Allemande Interdit le Piratage des Ordinateurs par la Police', Le Monde, 7 February 2007.

[23] Federal Constitutional Court judgment of 27 February 2008 (Cases 1 BvR 370/07 and 1 BvR 595/07).

blocks any websites of the political opposition, and set up a monitoring regime for civilian Internet users and Internet cybercafés. In Syria, the Assad government has engaged in extensive filtering of websites related to politics, minorities, and human rights[24], increasingly so since social media has played a crucial role in the Syrian uprising[25]. The "Syrian Revolution 2011" Facebook page, which by June 2012 had over 500,000 members from both inside and outside the country, has been a vital source of information for opponents[26]. The specificity of the Syrian context has been citizen journalists' use of mobile devices and video-sharing websites, which has become a platform to cover demonstrations and human rights violations of the Government, and to spread them to the world after most foreign correspondents were forced to leave the country. By March 2012, citizens posted to YouTube more than 40,000 video clips, many of which were rebroadcast by leading news channels such as Al-Jazeera, the CNN, and the BBC[27]. Two countries show quite different practices that deserve to be highlighted with respect to censorship and surveillance: China and Saudi Arabia.

According to the OpenNet Initiative (ONI), China has a special Internet police division[28]. In addition, it has established, on the recommendation of the Ministry of Education and the Communist Youth League, practices "to strengthen the ideological education of students and to better control the use of the internet on campus[29]". To implement its Internet surveillance, China also relies on the cooperation of major Internet operators to refine the operation of search engines to Chinese citizens, as shown by the agreements between China and Google to exclude key words considered to be dangerous for the Chinese authorities[30]. Western companies seeking to do business in China do not hesitate to practice self-censorship in order to access the commercial benefits of the Chinese market. Elliot Schrage, Vice

[24] Guy Taylor, 'After the Damascus Spring Syrians search for freedom online', Reason.com, February 2007. http://reason.com/archives/2007/01/29/after-the-damascus-spring (Last accessed: 30 March 2014).

[25] Further developments: 'Civil Movements: the Impact of Facebook and Twitter', Dubai School of Government, Vol. 1, n 2, May 2011. http://www.dsg.ae/portals/3/DSG_Arab_Social_Media_Report_No_2.pdf (last accessed: 30 March 2014).

[26] The Syrian Revolution 2011 Facebook Statistics,' Socialbakers.com. http://www.socialbakers.com/facebook-pages/420796315726-the-syrian-revolution-2011 (last accessed: 30 March 2014).

[27] Robert Mackey, 'Syria's Losing Battle to Control the News', The Lede, 13 March 2012.

[28] OpenNet Initiative, 'Internet Filtering in China in 2004-2005 : a Country Study'. https://opennet.net/studies/china (last accessed: 30 March 2014).

[29] Brice Pedroletti, 'Chine: Les Bons Petits Soldats de l'Internet', Le Monde, 7 Août 2008.

[30] Keith Bradsher, 'China Toughens Its restrictions On use of The Internet', The New York Times, 28 December 2012. See also the investigative report of Reporters Without Borders 'Journey To the Heart of Internet Censorship', October 2007. http://www.rsf.org/IMG/pdf/Voyage_au_coeur_de_la_censure_GB.pdf (last accessed: 30 March 2014).

President, Global Communications and Public Affairs of Google, clearly declared so in his testimony before the United States Committee on International Relations of the House Representatives:

> *"I'm here today to answer any and all questions you might have about how we are attempting to do business in China. I certainly don't – my colleagues certainly don't – expect everyone to agree with our decision to launch a new service inside this challenging, complex, promising market. I hope my testimony will help explain how we came to our decision, what we're seeking to accomplish, and how we're seeking to accomplish it. At the outset, I want to acknowledge what I hope is obvious: Figuring out how to deal with China has been a difficult exercise for Google. The requirements of doing business in China include self-censorship – something that runs counter to Google's most basic values and commitments as a company. Despite that, we made a decision to launch a new product for China – Google.cn – that respects the content restrictions imposed by Chinese laws and regulations. Understandably, many are puzzled or upset by our decision. But our decision was based on a judgment that Google.cn will make a meaningful – though imperfect – contribution to the overall expansion of access to information in China"*[31].

This is an often-used justification of self-censorship: that access to a market governed by an entity that restricts access to information will encourage its transformation from within to an entity that respects freedom of access to online information. What he does not say is that the financial weight of the Chinese market played a crucial role in the decision of companies like Google, Yahoo! or Microsoft, and has influenced their policy to comply with conditions that they would have rejected elsewhere. For instance such extreme measures are not taken with respect to smaller markets that also restrict content, such as Saudi Arabia and Iran. In the pursuit of lucrative markets, it is important to ensure that dangerous precedents such as the exclusive relationship with China do not become the norm. We should mention, however, that Google recently took the decision to encrypt search text in China and all over the world so that Internet users can avoid Government scrutiny and cyber surveillance, as a

[31] Elliot Schrage, Testimony of Google Inc. before the Subcommittee on Asia and the Pacific, and the Subcommittee on Africa, Global Human Rights, and International Operations Committee on International Relations, United States House of Representatives February 15, 2006. http://googleblog.blogspot.fr/2006/02/testimony-internet-in-china.html (last accessed: 30 March 2014).

"consequence of Edward Snowden's release last year of National Security Agency (NSA)32 documents detailing the extent of government surveillance of the Internet" [33].

Saudi Arabia has other concerns with respect to access to information, primarily concerning morality and religion. According to the study conducted by the ONI on Internet filtering in Saudi Arabia:

> *"Saudi Arabia publically acknowledges censoring morally inappropriate and religiously sensitive material, but the authorities also filter oppositional political sites and sites focused on human rights issues. In addition, the state has introduced new surveillance measures at Internet cafés and has announced plans to start a system that will require local sites to register with the authorities. Saudi citizens have started to use the Internet for online activism, but the authorities have arrested several online writers and blocked their content. A local human rights group expressed interest in legally challenging the government's censorship of human rights sites. Generally, Internet filtering in Saudi Arabia mirrors broader attempts by the state to repress opposition and promote a single religious creed"*[34].

Unlike Internet filtering in China, decisions, procedures and the philosophy of the Saudi system is quite transparent and explained clearly on its website, the Internet Service Unit[35] (ISU). If they try to access a banned site, users see a web page that informs them that the site is prohibited. More recently in Turkey, after passing a bill on February 2014 that would tighten government controls over the Internet, Turkish Prime Minister Tayyip Erdoğan threatened on 21 March 2014 to 'root out' social media (YouTube has already been banned after users criticising Kamal Atatürk) and to 'eradicate' the micro-blogging platform Twitter which is according to him, "the worst menace to society":

> *"The international community can say this, can say that. I don't care at all. Everyone will see how powerful the Republic of Turkey is," he said in a characteristically unyielding tone*[36]*"*.

[32] Ewen Macaskill, Gabriel Dance, 'NSA Files Decoded : What the Revelations Mean to You ?', The Guardian, 1 November 2013.

[33] Craig Timberg, Jya Lynn Yang, 'Google is Encrypting Search Globally. That's Bad For The NSA and China's Censors', The Washington Post, 12 March 2014.

[34] Open Net Initiative, 'Internet Filtering in Saudi Arabia', 6 August 2009. https://opennet.net/sites/opennet.net/files/ONI_SaudiArabia_2009.pdf (last accessed: 30 March 2014).

[35] Internet Service Unit, http://www.isu.net.sa/index.htm (last accessed; 30 March 2014).

[36] Declaration of Tayyip Erdoğan Citation taken from: http://www.huffingtonpost.com/2014/03/21/turkey-president-twitter-ban_n_5005759.html (last accessed: 30 March 2014).

With very little surprise, Twitter was blocked all over the country, on the grounds of the protection of national security[37]. In response, Twitter offered SMS to Turkish Twitter users who were quick to come up with their own ways to by-pass the block. The hashtag #TwitterisblockedinTurkey quickly moved to the top trending worldwide, which shows the power of the e-democracy: the banning moved beyond borders and protests to the ban started to rise all over the world, which may lead to pressures on the Turkish Government. In fact, the first 24 hours after the ban was introduced had the highest number of tweets to date from Turkish Twitter users.

At a time when China, Russia, Saudi Arabia, Sudan and the United Arab Emirates have allied to extend new governmental powers to regulate and control cyberspace[38] within their real-world borders, we observe that the growing online initiatives and communities do not follow national borders, and that many governments, including democracies (see Prime Minister David Cameron considering banning Twitter and Facebook during UK riots[39]), openly fear losing control over their online citizens. Hence, the global digital conversion brings new risks that have to be controlled, and a balance must be found. Indeed, while the Government has to protect its citizen from Internet abuses, the Internet must remain a free platform of civic expression for users, without any form of governmental restrictions.

5. Towards more adapted regulations?

With the emergence of new technologies, the demand for appropriate regulation is urgent in order to enhance the positive uses of the Internet and the control or prohibition of the negative ones. Online information environment and electronic communication must be respectful of individual freedoms. It cannot become a new jungle where the only fittest prevail. Therefore, social control of these technologies by the law is essential. This objective has justified the introduction of specific legislation regarding computers, telecommunications, electronic communications or video surveillance to organize the control without slowing down the expansion of the digital society. It is not only necessary to assert rights against the information society, but also to ensure the implementation of new regulations or new rights.

[37] Kevin Rawlinson, ‘Turkey blocks use of Twitter after prime minister attacks social media site’, The Guardian, 21 March 2014.

[38] Further information : Katherine Maher, ‘No, the U.S. Isn’t ‘Giving Up Control’ of the Internet’, Politico Magazine, 19 March 2014.

[39] Josh Halliday, ‘David Cameron Considers Banning Suspected Rioters From Social media’, The Guardian, 11 August 2011.

At the same time, the digital control of the e-society is not an easy task. It quickly appears as a constraint or censorship on the exercise of a new freedom. A real balance has to be found, as suggested by the press release of the deputy secretary general of the Council of Europe:

> "The Internet has a huge importance for economic, social and cultural development. It represents a critical global resource, and should be protected as such, including through international law. The Council of Europe is ready to do its part to contribute to an accessible, free, sustainable, robust and secure Internet"[40].

Hence, the contribution to the emergence of a real cyber-law appears to be urgent.

6. Rights and freedoms should be confirmed and refined in the digital space

New information technologies and communication have led to the adaptation of existing legislation or the adoption of new legislation. The global aim of this legislation is to introduce rules that organize online activities without blocking or banning. Nevertheless, there is always a lag between technical abilities and the time for legal measures to take hold. It is wise to incorporate general principles rather than detailed rules to ensure that the legislation does not become obsolete as technology changes. In all cases, individual rights and freedoms must always be affirmed or confirmed. Thus, technologies of information and communications require a high level of protection of individual rights. Digital society should be properly regulated in order to grow and produce the best democratic, cultural, social and economic benefits. It must respect fundamental rights. In 2009, a recommendation of the European Parliament stated:

> *"Whereas the host of fundamental rights that are affected in the Internet world include, but are not limited to, respect for private life (including the right to permanently delete a personal digital footprint), data protection, freedom of expression, speech and association, freedom of the press, political expression and participation, non-discrimination, and education; whereas the content of such rights, including their field of application and their scope, the level of protection provided by such rights and the prohibitions on abuse of such rights should be governed by the rules on the protection of human and fundamental rights guaranteed by the Constitutions of the Member States, international human rights treaties,*

[40] Statement by Maud de Boer-Buquicchio, Deputy Secretary General. Opening of the UN Internet Governance Forum in Hyderabad, India, 02 December 2008. https://wcd.coe.int/ViewDoc.jsp?Ref=PR865(2008)&Language=lanEnglish&Ver=original&Site=DC&BackColorInternet=F5CA75&BackColorIntranet=F5CA75&BackColorLogged=A9BACE (last accessed: 30 March 2014).

> *including the ECHR, general principles of Community law and the Charter of Fundamental Rights of the European Union, and/or by other relevant rules of national, international and Community law, in their respective fields of application"*[41].

This requires good governance and good control of the Internet both in the States and Europe as well as throughout the world. It requires good coordination and harmonization of the law of the Internet that embodies its international dimension. Subsequently, it is essential to ensure system security, and finally, to seek the right levels of governance and Internet regulation. Indeed, we must never forget that the Internet is a network that knows no state borders, and that national law must be consistent with international law to meet global challenges. The Internet should be treated as a laboratory for new forms of governance that oblige cooperation between national and international decisions. International cooperation should promote regulation, including preventing excessive development of informatics havens. At each level, principles should be created in order to develop the information regimes in every State.

The United Nations, its member states, and the International Telecommunication Union (ITU) established a *World Summit on the Information Society* (WSIS) which has been held in Geneva in 2003 and in Tunis in 2005. The summit adopted an important declaration of principles: *Building the Information Society: a Global Challenge in the New Millennium*[42]. This declaration establishes a general framework for the development of the information society in coherence with the Universal Declaration of Human Rights, for example with regard to freedom of opinion, freedom of expression and free and full development of personality and the right of access to new technologies for all. The goal is to found the information society on fundamental principles as article 19 of this declaration advocates:

> *"We are resolute in our quest to ensure that everyone can benefit from the opportunities that ICTs can offer. We agree that to meet these challenges, all stakeholders should work together to: improve access to information and communication infrastructure and technologies as well as to*

[41] European Parliament recommendation of 26 March 2009 to the Council on Strengthening Security and Fundamental Freedoms on the Internet.

[42] World Summit on the Information Society, Declaration of Principles Building the Information Society: a global challenge in the new Millennium, 12 December 2003, document WSIS-03/GENEVA/DOC/4-E. http://www.itu.int/wsis/docs/geneva/official/dop.html (last accessed: 30 March 2014).

> *information and knowledge; build capacity; increase confidence and security in the use of ICTs; create an enabling environment at all levels; develop and widen ICT applications; foster and respect cultural diversity; recognize the role of the media; address the ethical dimensions of the Information Society; and encourage international and regional cooperation. We agree that these are the key principles for building an inclusive Information Society".*

This clearly shows the urgent need for international regulation of the Internet and its uses in connection with the global nature of the network. But international law intervention is far from easy, given the construction of the global network. The network of networks is still largely dominated by the *Internet Corporation for Assigned Names and Numbers*[43] (ICANN) a California private company that manage domain names. This status is reflected in the resolution of the summit in Tunis that called for a forum for dialogue, and an enhanced cooperation between European Union member states without questioning the quasi-monopolistic role of the ICANN. But on 14 March 2014, the United States leaned towards an international governance of the Internet and accepted that the ICANN does not remain supervised only by the US government. This is a strong political decision which indirectly results of the consequences of the Snowden Affair and the NSA surveillance scandal. The United States agreed to waive their direct control over the main body of Internet governance.

This massive change leads to two major consequences regarding Internet regulation and e-democracy. Gene Kimmelman, president of Public Knowledge, a group that promotes open access to the Internet, considers that this decision

> *"Is a step in the right direction to resolve important international disputes about how the Internet is governed".*[44]

First, this would mean the end of the US monopoly over rules governing domain names ICANN will be able to leave the American fold and become a multi-stakeholder organization. Second, if the United States continues to hold a significant and special role in the management of ICANN, this reform is indicative of a trend towards an internationalization of the Internet. However, it remains to determine whether the ICANN reform will actually be implemented transparently. The road is still long until real and

[43] Further information: https://www.icann.org/en/about (last accessed: 30 March 2014).

[44] Craig Timberg, 'U.S. to Relinquish Remaining Control Over the Internet', The Washington post, 14 March 2014.

efficient global Internet governance or even international cyber law, and its implementation will require efforts and involvement from all international actors. Finally, powers currently given to ICANN will not be challenged, but the challenge now is to determine the conditions for an international control of the action of this authority. Thus, in order to be effective, ICANN has yet to develop a transition plan in collaboration with other stakeholders in this critical infrastructure. In this context, and following the declaration of the US Department of Commerce, Fadi Chehadé ICANN's President and CEO convened actors of the global Internet community in Singapore on 23-27 March 2014[45]

> *"To join us [ICANN] in developing this transition process. All stakeholders deserve a voice in the management and governance of this global resource as equal partners"*[46].

If ICANN still has a long way to go and if this transition must lead to a deep reform, we can only hope that this (still very controversial) institution will be deeply be transformed into a form of 'super regulator', a sort of United Nations Organization of the Internet where all actors can get together to become the safeguards of the web.

Europe has addressed this issue with the adoption of many texts, not only within the frame of the Council of Europe but also within the European Union. The Council of Europe has adopted several conventions and on computers, personal data protection issues or the Internet. In 1981, a *European Convention for the Protection of Individuals With Regard to Automatic Processing of Personal Data* was carried out to engage member states to take necessary precautions. For example, in France this convention entered into force in 1985 and complements the provisions of the law of 1978 on *Information, Technology, Data Files and Civil Liberties*. In addition, this convention also holds an enhanced European cooperation in this area. In 2001, a Convention on Cybercrime was adopted by the Council of Europe to fight against cyber crime in cyber space. It facilitates better cooperation between member states and encourages the adoption of appropriate legislation regarding this matter.

[45] See ICANN Singapore GAC Communiqué, 27 March 2014 : http://www.icann.org/en/news/announcements/announcement-27mar14-en.htm (last accessed: 30 March 2014).

[46] ICANN Press Briefing Scheduled with Board Chair and CEO,14 March 2014 : https://www.icann.org/en/news/press/releases/release-14mar14-en ((last accessed : 30 March 2014).

As for the European Union, it has developed a specific law to promote the development of the Internet safe and respectful of human rights[47]. The general spirit of the institutions of the European Union on the regulation of the Internet is to achieve secure and unreservedly access to secure Internet, to fight cybercrime and to achieve protection of individuals and promotion of fundamental freedoms on the Internet.

7. Towards a democratic online citizenry?

The conditions for the emergence of a democratic online citizenry include the following:

- *The need for recognition of a fundamental right of access to the digital space*. The digital Republic implies the recognition of a fundamental right of access to the digital space to avoid the risk of a digital divide[48]. Indeed, the benefits of a digital society are real if IT tools are widely distributed and made available to the greatest number. But, if the e-society and its positive effects are reserved only for a certain part of the population, a digital divide will emerge, with in the one hand, ordinary citizens, and on the other hand, an elite of e-citizens. Indeed, e-democracy will be a relevant innovation only if a very broad number of citizens can use it without restrictions.

- *The necessity of constructing a new fundamental right of access to digital networks*. Government policies have been implemented over the past 20 years to develop digital networks, first with the development of telecommunications, electronic communications and then to technically facilitate Internet access.

[47] For example: Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, 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 (Directive on privacy and electronic communications), Directive 2003/98/EC on the re-use of public sector information, Council Framework Decision 2005/222/JHA of 24 February 2005 on attacks against information systems, the Communication from the Commission to the European Parliament, the Council and the Committee of the Regions of 22 May 2007 – Towards a general policy on the fight against cyber crime, or the Council Framework Decision 2008/919/JHA of 28 November 2008 amending Framework Decision 2002/475/JHA on combating terrorism.

[48] Further developments on digital divide: Lee Rainie, 'The State of Digital Divide' 5 November 2013, Pew research Internet Project: http://www.pewinternet.org/2013/11/05/the-state-of-digital-divides-video-slides/ (last accessed 30 March 2014).

This is also the goal of the European Union Institutions and the Council of Europe. The European Parliament explained so in its recommendation of 26 March 2009:

> *“The Internet can be an extraordinary opportunity to enhance active citizenship and that, in this respect, access to networks and contents is one of the key elements; recommend that this issue be further developed on the basis of the assumption that everyone has a right to participate in the information society and that institutions and stakeholders at all levels have a general responsibility to assist in this development, thus attacking the twin new challenges of e-illiteracy and democratic exclusion in the electronic age”*[49].

This recognition would follow the thinking of former Secretary of State Hillary Clinton, who called for:

> *“Internet freedom as fundamental as free speech itself, saying cyberspace is the 21st century town square where governments need to find a balanced way to preserve universal principles such as liberty, transparency and free expression. The freedoms of expression, assembly, and association online comprise what I have called the freedom to connect”*[50].

But the recognition of a new fundamental right of access to networks and to the Internet is not sufficient in itself. It is also necessary to move towards the creation of tools, organizations, and regulations to facilitate this environment, through the implementation of the right to digital education and access to digital culture, in order to implement equality between online citizens.

Conclusion

Cyber citizenship is at the service of democracy because it allows actions that would be impossible without cyberspace: freedom of expression without limits or borders, a regular citizen web presence, individual or collective contributions to forums, the emergence of a collective intelligence, the denunciation of authoritarian regimes on a global scale, and the reporting of violations of rights and freedoms. Hence, direct democracy or participatory

[49] European Parliament recommendation of 26 March 2009 to the Council on Strengthening Security and Fundamental Freedoms on the Internet (2008/2160(INI)) (§W (1) b).

[50] Michael Martinez, ‘Clinton Calls for Global Recognition of Internet Freedom’, CNN, 16 February 2011.

democracy is possible through the Internet. But at the same time, the web has become a gigantic instrument that allows the control and monitoring of our actions on the Internet and constitutes a threat to our rights and freedoms. High-tech surveillance is organized, including when it is justified by good reasons, like fighting cybercrime. Therefore, it seems urgent to take into account the changes of democracy in a digital environment, so that it actually contributes to the emergence of a true cyber citizenship and ensure to recognize effectively at both national and supra-national, a real constitutionalized fundamental right to access the Internet, which will allow not only a more efficient protection of the individuals by the State, but also - and perhaps especially – to promote and guarantee the e-democracy as a tool serving the rights and freedoms of the emerging and rising *homo numericus*.