Law, Governance and Technology Series 7

Giovanni Ziccardi

Resistance, Liberation Technology and Human Rights in the Digital Age

Springer

Resistance, Liberation Technology and Human Rights in the Digital Age

Law, Governance and Technology Series

VOLUME 7

For further volumes:
http://www.springer.com/series/8808

Giovanni Ziccardi

Resistance, Liberation Technology and Human Rights in the Digital Age

Springer

Giovanni Ziccardi
Department “Cesare Beccaria”
Faculty of Law
University of Milan
Milano, Italy

ISBN 978-94-007-5275-7 ISBN 978-94-007-5276-4 (eBook)
DOI 10.1007/978-94-007-5276-4
Springer Dordrecht Heidelberg New York London

Library of Congress Control Number: 2012949676

Printed on acid-free paper

Springer is part of Springer Science+Business Media (www.springer.com)

Contents

Chapter 1
Opening Remarks: Hacking and Digital Dissidence

1.1 Using Computers for the Pursuit of Political and Social Changes and for the Benefit of All Mankind

The concrete possibility of using all the various types of technologies available to mankind for the specific purposes of networking, of contributing to political and social changes and of contrasting oppressive dictatorships, and even authority in general, has always been, since the very first activities of university hackers[1] in California during the 1960s, a singularly fascinating and often inspiring issue.[2]

[1] In this book I will use the term "hacker" *exclusively* to indicate subjects with great computer skills, or dedicated to a creative use of technology, *without* criminal intentions. To indicate criminal activities carried out with the help of the computer, or against a computer system, I will use the expression "computer criminals". For a preliminary historical overview of hacking and the first Internet projects see, *inter alia*, Rosenzweig's essay concerning "wizards, bureaucrats, warriors and hackers" (Rosenzweig 1998). The author outlines how the profound and complex development of the Internet cannot be divorced from the idiosyncratic and personal visions of those scientists and bureaucrats whose sweat and dedication launched the project, and made it real. He identifies those hackers as originating from *three* different frameworks: (i) from the social history of the field of computer science, (ii) from the Cold War scientific and technical apparatus, which took advantage of massive government funding for computers and networking as tools for fighting nuclear and conventional wars, and (iii) from the countercultural radicalism that sought to redirect technology toward a more decentralized, and non-hierarchical, vision of society (Rosenzweig 1998: 1552).

[2] Among the many sources, including books, academic essays, documentaries and movies that describe the activities of the hackers in California in the 1960s, 1970s and 1980s, the reader might like to consider the following: *Triumph of the Nerds: The Rise of Accidental Empires* (1996), an influential documentary written and directed by Robert X. Cringely; the movie *Pirates of Silicon Valley* (1999), directed by Martyn Burke, based on an accurate Freiberger and Swaine book (Freiberger and Swaine 2000), the documentary *In Search of the Valley*, profiling many of the founders of the so-called *Silicon Valley*, and the book by Livingston on the "founding fathers" of the information technology world (Livingston 2007). See also the interesting Pfaffenberger's critical approach regarding the *non revolution* of personal computer revolution (Pfaffenberger 1988): the scholar remarks that for the phone phreakers, hackers, and (later) early personal computer users "the goal was not to overthrow the *System*, but rather the more conservative aim of gaining entry

G. Ziccardi, *Resistance, Liberation Technology and Human Rights in the Digital Age*, Law, Governance and Technology Series 7,
DOI 10.1007/978-94-007-5276-4_1, © Springer Netherlands 2013

The idea that computers might not only assist humans, but might also allow the most complete expansion possible of intellectual and cognitive capacities and the widest and most transparent diffusion of information useful for *progress* and *democracy* (Turner 2005), first took root in the theories of the protest movements that flourished in North America in the 1960s[3] and, in particular, formed the basis of the ideas of, among others, Lee Felsenstein, the *Free Speech Movement* and the first California homebrew computer clubs (Lash 2006; Turner 2006).

Concerning the interpretation of the role of computers by Lee Felsenstein, and the possibility of *giving power* to individuals not only over *machines* but also, and even more importantly, over *political oppressors*, Levy is quite unequivocal. The author outlines how Felsenstein considered the computer itself a *model for activism*, and hoped the proliferation of computers to people would spread a sort of *hacker ethic*[4] throughout society (Levy 1984: 142).

Wozniak, the co-founder of *Apple Computers*, wrote in detail about the importance of the digital revolution and the urgency of controlling computers. This hacker describes how, in the 1970s, the small, but quickly growing, computer scene was based on the belief that all the hackers were on top of a *revolution*. Hackers, and the people, were finally going to get control of their own computers, despite the fact that computers, until that time, belonged only to million-dollar companies (Wozniak 1984).

The motto *a computer for all*, and the urgency that those early intellectuals felt regarding the development and penetration of inexpensive, mass-market computers that could be easily accessible to *everyone* were the theories that, for the first time, focused consideration on the radical idea that technology might, in fact, *improve the world* (Levy 1984).

It seems to me that there is a very clear *common thread* connecting those first stimulating ideas of the 1960s with events occurring now in different parts of the world, where various technology platforms are becoming fundamental support tools for individuals who not only need to seek knowledge beyond state filters, but who also see, in these new technologies, an opportunity to *seek freedom* in contexts that tend to limit it.

Hauben elucidated this shift, remarking that some of the people who were involved in student protests continued their efforts to bring *power to the people* by developing and spreading computer power in forms that were more accessible and affordable for individuals (Hauben 1996).

---

to the *System*, helping to improve it, and ultimately gaining prestige and self-esteem by winning its approval" (Pfaffenberger 1988: 41). The author's conclusions are clear: personal computing has become *impersonal computing*, in which the machine, that was supposed to foster autonomy and individual creativity, is reduced to serving as a mere mainframe terminal (Pfaffenberger 1988: 47).

[3] See Searle's studies regarding *campus wars* (Searle 1971), the movie *Berkeley in the Sixties* (1990) and the article by Hauben on *participatory democracy* and online activities (Hauben 1996). As Turner notes, both the *New Left* and the counterculture hoped to transform the technocratic bureaucracies that, in their view, had brought Americans the Cold War and the conflict in Vietnam (Turner 2005: 493).

[4] See Sect. 3.7.

According to this scholar, three steps can be identified:

1. *the first step is the creation of the PC*. The personal computer movement of the 1970s, first of all, created the personal computer;
2. *the second step is the mass production and diffusion of affordable computers*. By the mid 1980s, protest movements forced corporations to produce computers which everyone could afford;
3. *the third step is the birth of the Internet*. Finally, Internet, a brand new communication *medium*, grew out of the ARPANET research that started in 1969.

These communications advances, outlines Hauben, coupled with the widening availability of computers, transformed the spirit of the 1960s into an achievable goal for modern times (Hauben 1996); in fact, in modern times, there are indeed thousands of *digital dissidents* around the world who risk their liberty to protest and to oppose repressive forms of government and strategies aimed at controlling the behavior of the population.[5] Relying on little else but their own quick thinking and, often, on obsolete technologies, they are threatened and detained for the opinions they express and the news they divulge; dedicated to the development of techniques to circumvent surveillance and filter technologies and to hide, encrypt, anonymize and disclose information, they are constantly tracked by the authorities of their countries. Using smartphones,[6] cameras,[7] laptops and handheld video cameras, they transmit in real time the facts of the societies in which they live. They act to eradicate filters; they fight to tear down codes of silence and to elude censorship software; they refute the theory of *secrecy* surrounding matters of public interest, while prizing it above all else in their own private lives; they aim to erode media monopolies and to disprove false state truths. They create web sites to divulge

[5] See the study by Warf and Grimes regarding *counterhegemonic discourses* and the Internet (Warf and Grimes 1997): the authors identify the Internet as a terrain of contested philosophies and politics and of confrontation, and a place that can also sustain counterhegemonic discourses, challenging established systems of domination, legitimating and publicizing political claims by the powerless and marginalized. Increasingly easy access to the e-mail and the web allows many politically disenfranchised groups to reach three important targets: (i) communicate with like-minded, or sympathetic, audiences, (ii) publicize causes often overlooked by the mainstream media, and (iii) offer perspectives frequently stifled by the conservative corporate ownership of newspapers, television, and other media outlets (Warf and Grimes 1997: 260).

[6] An interesting introductory study regarding the use of mobile phones for the purpose of resistance in Belarus and Serbia was written, *inter alia*, by Miard (2009). For a global overview see, also, the work by Heinzelman, Brown and Meier concerning the use of mobile technology in *crowdsourcing* and *peace mapping* contexts (Heinzelman et al. 2011), Salazar and Soto on the Mexican experience of monitoring elections and crowdsourcing (Salazar and Soto 2011) as well as the research by Korenblum and Andemariam related to cellular phones use in conflict zones (Korenblum and Andemariam 2011).

[7] See, *inter alia*, an essay by Whitty regarding soldier photography of detainee abuse in Iraq (Whitty 2010). See Sect. 2.3.2.4.

reserved documents, and update blogs with the sole aim of making the world more transparent.[8] Last, but not least, they write complex source code, honing their skills daily, with one single mission: *resistance*.

The common thread, mentioned above, thus comes even more sharply into focus: these *activists* constitute a new breed of *hacker*, and they are among the few who rightly deserve the name today. They are bringing back the groundbreaking ideas of the 1960s, renewing and invigorating the theories of those first digital rebels, adapting them to the modern world and passing them on to future generations in forms that are increasingly fascinating and innovative. They outwit technological barriers imposed by authorities and corporations, attack global surveillance systems, fight for cultural and artistic liberties and for the free flow of ideas, invest time and effort to create network architectures which safeguard user anonymity, program and divulge free source code, and seek to force states to adopt systems that are more transparent, and not arbitrarily and covertly controllable.

Their plans are clear: they seek to change the world using nothing more than computers and networks; they aim to topple traditional political systems and bureaucracies, and to expose corruption.

These activists freely share all they discover; they are quite different, in the ways they think and act, from the so-called hackers whose criminal behaviors have contributed to the contamination of one of the most noble chapters in the history of computer science.

Sterling was one of the first scholars to clearly explain the true nature of the term *hacker* (Sterling 1992).

He highlighted several elements: the free-wheeling intellectual exploration of the highest and deepest potential of computer systems, the determination to make access to computers and information as *free* and *open* as possible, but also the heartfelt conviction that *beauty* can be found in computers, and that the fine aesthetic in a perfect program can liberate the mind and spirit. Sterling remarks that the term *hacker* has had an unfortunate history, but hackers of all kinds are absolutely soaked through with heroic anti-bureaucratic sentiment. They are, the writer says, *the postmodern electronic equivalent of the cowboy and mountain man* (Sterling 1992: 37–38).

Soon, however, this common perception of hacking as a noble and harmless activity underwent a significant change.

There was a diffusion of the idea of the hacker, Sterling writes, as a sociopath without responsibility, a criminal, a subverter and manipulator of telephone systems, to the point that today the term *hacking* is routinely used by law enforcement officials to refer to computer fraud and abuse (Sterling 1992: 38). Sterling, again, outlines how any form of power without responsibility, without direct and formal checks and balances, is *frightening* to people, and hackers *are* frightening (Sterling 1992: 38).

[8] A striking Egyptian case involved Khaled Said, a young boy killed by Egyptian police in 2010. The scene was captured with a mobile phone; the resulting photos, once they were circulated, raised vocal protests worldwide that led to the arrest of the perpetrators of the brutal police action (Etling et al. 2010: 3).

The basis of this fear, the scholar explains, is not irrational, because fear of hackers goes well beyond the fear of merely criminal activity: subversion and manipulation of the phone systems is an act with disturbing political overtones, and, in America, computers and telephones are potent symbols of *organized authority* and the technocratic business élite (Sterling 1992: 38).

From a social and political point of view, the scholar notes that there is an element, in American culture, that has always strongly rebelled against organized authority and technocratic business élite symbols, and against all large industrial computers and all phone companies. Sterling writes of a certain *anarchical tinge* deep in the American soul that delights in causing confusion and pain to all *bureaucracies*, including technological ones. There is sometimes malice and vandalism in this attitude, the author remarks, but it is a deep and cherished part of the American national character: the outlaw, the rebel, the rugged individual, the pioneer, the sturdy Jeffersonian yeoman, the private citizen resisting interference in his pursuit of happiness are all figures, Sterling enumerates, that all Americans recognize, and that many will strongly applaud and defend. The essence of hacking, according to this writer, is strictly connected to all these activities (Sterling 1992: 38).

Digital dissidents, by contrast, engaging in a new and extremely compelling form of hacking, carry out their battles in silence, through small actions, which must often be considered collectively in order to fully appreciate their vital (and *viral*) importance: they moderate forums, energize discussion groups, reconfigure remote servers in a matter of minutes in the name of activism, write source code and send it to other dissidents, perhaps far away, still in their home countries, isolated behind state firewall systems.

They act, maintaining low profiles, sometimes even in secrecy, until they manage to constitute so many pieces of a mosaic which only slowly takes form, but which represents one of the last strongholds in the defense of civil liberties in the modern age.

1.2 From Early Hackers to Digital Resistance Activities

The evolution from the *ideas* that are at the basis of these new hackers' activities to actual digital resistance, i.e. a *strategy* aimed at unlocking the structure of a corporation, of a state, of a single computer or even of an entire legal or political system for the purpose of benefitting humanity, is one of the most interesting aspects of communication technology in the modern world.

Clearly, the more effective a single action of digital protest is, the more it will be apparent that all misguided political and legal initiatives, projects aimed at censorship, state filters and systems controlling Internet and social media will be destined to fail even before they are fully implemented: the identification of system weakpoints and of loopholes in flawed legislation framework is facilitated, and in some cases demanded, by technology.

These sorts of activities have already been defined as *Digital Resistance*,[9] *Electronic Civil Disobedience*[10] or activism related to the use of *Liberation Technology*[11]: they denote a new form of civil resistance, which has, at its core, the fusion of traditional resistance tactics with the skilled use of newly available technology.

As Diamond sapiently notes, liberation technology means any form of information and communication technology able to expand political, social, and economic freedom. In modern times, it embraces essentially the most advanced, interrelated forms of digital technologies, like the computer, the Internet, the mobile phone, and countless innovative applications for them, including new social media such as *Facebook* and *Twitter* (Diamond 2010: 70).

While it is mistaken to maintain that digital resistance activities are necessary only in those countries where repressive regimes engage in political practices that are distant from the democratic standards enjoyed in other nations, it is also clear that, in these more oppressive states, the process of rebellion will be more evident (and more strongly motivated), and will often take on forms that are more aggressive, resulting in more violent repression.

Even in so-called "democratic states", however, there are current political initiatives aimed at limiting citizens' liberties and the possibility of communicating (and of uncovering) facts which directly involve them; there are projects, today, aimed at obscuring public sector activities, at masking corruption, at hindering the full performance and implementation of fundamental procedures and processes. Careful attention to all that occurs, making the best use of new technologies, is not only beneficial, but even of critical importance in every kind of society and under every form of government.

Political systems which base their powers on barriers, on the willingness to place their own intangible moral and cultural values under a glass bell in order to prevent them from being *contaminated* by the free flow of information, are destined to cede and to become increasingly transparent in their actions.

---

[9] See the *Critical Art Ensemble* definition of the term *digital resistance* (Critical Art Ensemble 2001, 2000), the studies by Hands concerning dissent, resistance and rebellion in a digital culture (Hands 2001) and by Russell exploring digital resistance issues (Russell 2005). See, also, Sect. 2.3.2.3.

[10] See the *Critical Art Ensemble* definition of the concept of *electronic civil disobedience* (Critical Art Ensemble 1995), the studies by Wray on the some topic (Wray 1998) and by Klang on online digital disobedience (Klang 2004). Klang outlines, in his study, several *criminal activities* which are used as active forms of Internet based protest. The author describes actions such as *unsolicited e-mail* (and whether a political protest message can fall under the definition of *communication* for the purposes of direct marketing), *e-mail bombing* (and the possibility of limiting the legitimate user's access to or use of a computer system, with criminal consequences), *hacking*, *web page defacement* and *denial of service attacks* (Klang 2004: 75, 76, 77).

[11] See the interesting definition of *liberation technology* by Diamond: a *tool* that enables citizens to report news, expose wrongdoing, express opinions, mobilize protest, monitor elections, scrutinize government, deepen participation, and expand the horizons of freedom (Diamond 2010: 70).

The introduction, in authoritarian and repressive environments, of content considered to be culturally improper or unacceptable will be increasingly difficult to avoid, as will the diffusion of reserved information from the confines of such nations. This will result, as it nearly always has, in increased pluralism and democracy, culture and innovation, liberty and new stimuli, but also, in some cases, in violent reactions and in systematic violations of human rights.

1.3 The So-Called *Twitter Revolutions*

It may be going too far to maintain that the beneficial aspects of this type of progress are made possible *only* by hackers and solely through the diffusion of new technologies, or by the proliferation of the so-called *Twitter Revolutions* (Morozov 2011); it is undeniable, however, that hacking, over the last 60 years of technological progress, has made fundamental contributions to the creation of an unprecedented framework of digital liberties.

Politics has never been able either to *satisfy* the real needs of Internet users or to *fully comprehend* the nature of the Internet, nor has does it seem to understand what might be the best rules and regulations to govern the Internet and to protect civil rights in cyberspace.

Attempts to "gag" web sites by extending the application of rules created for the press, often carrying significant limitations, in order to eliminate anonymity, unquestioningly incrementing instances of defamation and to impose the right to oblivion, along with the crusades on the part of certain politicians to "bring legality online"[12] are nothing more than justifications for proposing legislation aimed at diminishing the level of liberty.

The dream of absolute transparency is becoming, in these days, a reality, albeit one fraught with a number of inherent difficulties,[13] including those related to public and national security, which must be addressed and overcome, and which are already creating useful *antibodies* in both web users and in the overall social framework as well. There will certainly be an increasingly downward movement of political activities, toward the local, grassroots and even individual levels, despite the fact

[12] Purely as an example, see the two main provisions of a censorial draft law proposed in Italy in 2009, and fortunately dismissed, although the same *ratio* is recognizable in many other proposals, by an Italian Deputy, On. Gabriella Carlucci, aiming to make Internet the "land of freedom, rights and duties". The text of the bill is: "It is forbidden to publish online or to facilitate the transmission over the Internet of content in any form (text, sound, audiovisual and information technology, including databases) *anonymously*" (Article 1), and "With regard to the offenses of defamation, all rules relating to the press apply, without exception" (Article 2). Italian Draft Law Proposal n. 2195. http://www.camera.it/126?Pdl=2195. Accessed 18 October 2011 (translation by the author).

[13] See Lessig's interesting remarks on *radical transparency* (Lessig 2009), and the study of Bannister and Connolly regarding the perils of openness in e-government (Bannister and Connolly 2010).

that the majority of institutions and organized groups are loathe to accept real transparency with regard to internal procedures.[14]

On the other hand, it is also apparent that the advent of an ever-increasing range of communication *encryption* technologies is of growing concern to law enforcement agencies throughout the world. It is inconceivable, for authorities, that should exist areas that are *non-interceptable*, in which it is possible to communicate in secret and in which users are truly anonymous. It is foreseeable, in the not so distant future, that there may be concerted attempts to seek to intensify, ostensibly for reasons of national security, control of these *grey areas* which so worry governments and in which, perhaps paradoxically, citizens' digital liberties are most fully manifested. This increased government control may well lead to the creation, in reaction, of true off-shore data heavens hosting the ideas and documents of all those who feel the need to continue to communicate within similar *grey zones*.

In addition to the analysis of the relationship between digital resistance activities and human rights (digital dissidence activities so often serve to reveal some of the most violent human rights violations), it is also particularly interesting to analyze the *levels* of digital liberty in several regions of the world, taking into consideration those laws and technologies which seek to limit the free expression of human rights.

The panorama which emerges from this type of analysis is quite worrisome: as technological evolution progresses, so at the same time do government investments seeking to *control* these new technologies. A map of government actions aimed at limiting digital liberties, and of the local digital resistance activities working against them, paints a very realistic portrait, which in some areas of the world is quite dire indeed.

Finally, a concrete analysis of the digital resistance techniques best suited to delicate contexts allows us to appreciate, once again, the geniality of those individuals who are forced to utilize technology, often in unconventional ways, to identify escape routes in contexts where human rights are limited and voices are stifled.

Three aspects, collectively, make up the focus of the main portion of this study:

1. the evolution of the concept of digital liberty, and its relationship with human rights;
2. the *level* of digital liberties and their protection throughout the world; and
3. the technologies which might help Internet users to change the *status quo* and to resist, in many cases, to oppressive laws.

[14] See, *inter alia*, Peckham's interesting study concerning the conflict between *Scientology*, the secret of publications and its Internet critics (Peckham 1998). The author correctly notes that the *radical democracy* of the Internet places more importance on popular opinion and attempts to sway disinterested bystanders. Peckham observes that, since the real authority of the Internet lies in the strength of numbers and popular appeals, the *struggle for popular legitimacy* is more important for on-line movement/countermovement conflict than lobbying a government for legislation. If a movement is to meet its goals on the Internet, the scholar writes, then it must appeal to the only real authority that exists: *Internet users* (Peckham 1998: 321).

1.4 The Worldwide Scenario, and Some Preliminary Interpretative Questions

Scholars who, moving from the general considerations mentioned above, desire to undertake a more methodical and in-depth analysis of the challenging issues surrounding the matters of digital dissidence, resistance and human rights in the era of Internet, and who desire to do so not only taking into account, but also seeking to interpret, the diverse issues, components and dichotomies that comprise this field, are faced with considerable difficulty.

There is, first of all, a multiplicity of intertwined issues, ranging from concrete dissident activities as they are carried out *in loco* to the most innovative hacking techniques used to communicate and to circumvent censorship, monitoring and surveillance worldwide.[15]

Legal and regulatory frameworks more or less restrictively denote specific geographical areas (nations labeled *enemies of Internet*, and others that continue to be *under observation*[16]), alongside the intricate complexities of defining legal and moral confines between protest, hacking, and criminal behavior.

This global framework is not only new, but also surprisingly multifaceted, and, at the same time, may often be difficult to pin down and even more difficult to interpret. Thus, it may be useful, as a preliminary approach, to first identify a few of the difficulties that face researchers approaching this field, so that we may then seek to address them in the course of the present study.

The first of these difficulties can be loosely defined as *geographic* or, in five senses, *global* (Pattaro and Sartor 2002), and the problems facing the scholars are not trivial. Such five fundamental aspects are:

1. the Internet is global since it concerns a significant, and increasing, share of the world's population (Pattaro and Sartor 2002: 1–2);
2. the Internet is global in regard to the geographical distribution of its users, who inhabit every country of the world, though enormous diversities in the penetration rates in different countries (Pattaro and Sartor 2002: 1–2);
3. the Internet is a global phenomenon since its distributed architecture allows in principle everyone of its nodes, and therefore every part of the world, to be both a *provider* and a *user* of global information (Pattaro and Sartor 2002: 1–2);
4. the Internet is global being one of the main causes of globalization. Thanks to the Internet, physical distance becomes irrelevant to communication, a global space

[15] Consider, for example, the *global surveillance* controversy generated by the *Echelon* project (Radden Keefe 2005). See, also, the European Parliament report on the existence of a global system for the interception of private and commercial communications at the address http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+REPORT+A5-2001-0264+0+DOC+XML+V0//EN. Accessed 6 November 2011.

[16] As stated by *Reporters Sans Frontières*, http://en.rsf.org/IMG/pdf/Internet_enemies.pdf. Accessed 22 October 2011.

is realized where personal interactions and organisational structures may be distributed all over the world, regardless of physical proximity (Pattaro and Sartor 2002: 1–2);

5. the Internet is a global phenomenon in the sense that it involves every sector of human activity. Not only in cyberspace individuals reproduce those activities that are used to perform in physical space, but the Internet is modifying the way in which all activities are carried out, from scientific research, to production, to socialization. Cyberspace merges with physical space, providing the substrate for a new type of social organization (Pattaro and Sartor 2002: 1–2).

It is well known that a plethora of digital technologies and tools are by now available worldwide, but it is somewhat less well known that there are enormous differences, both in relation to their *real availability* and to the ease of *obtaining* them (this difference is often referred to as the *digital divide*[17]) and, even more interesting for the current analysis, in relation to the effective use of these technologies on the part of "normal" individuals, even in those cases where technology is widely present.

There are states that, for various motives, nearly always economic and social, have very low percentages of Internet use among their citizens. This state of affairs exists because either the technology is simply not yet available, or has not yet physically reached the territory (sometimes these areas do not have electric power or running water either: consider certain nations of sub-Saharan Africa or the mountainous regions of Tibet, which, for clear geographic and topographic reasons, are extremely

[17] For a preliminary definition, and an illuminating introduction, on key issues related to the digital divide, see the study by Guillén and Suárez concerning the economic, political and sociological drivers of cross-national Internet use (Guillén and Suárez 2005). They provide a brief explanation of the causes of digital divide: differences in Internet use across countries are fundamentally related to economic variables, such as *pro capita* income and the cost of access (Guillén and Suárez 2005: 682). Interesting, also, is Wallsten's analysis of regulation and Internet use in developing countries and the *gap* between rich and poor countries in the diffusion of information technology, especially Internet access (Wallsten 2005). The section concerning Internet Service Providers (ISPs) regulation is quite topical: the author remarks that countries that require ISPs to get formal approval before beginning operations, have fewer Internet users and Internet hosts (Wallsten 2005: 519). See also Hatem Ali's study on the power of social media in developing nations (Hatem Ali 2011), Graham's considerations regarding the *spatialities* of the digital divide (Graham 2011) and Warschauer's remarks on digital divide in Egypt (Warschauser 2003). The study by Coeur De Roy concerning the African challenge (Coeur De Roy 1997) highlights the importance of electronic communication networks in encouraging the development processes in Africa. For a more focused overview on typical digital divide issues, see Attewell's study concerning the first and second digital divide (Attewell 2001), Natriello's essay regarding the contribution of the sociology of education in bridging the second digital divide (Natriello 2001), the Wagner, Bundorf, Singer and Baker study concerning free Internet access, digital divide and *health information* (Wagner et al. 2005), Hyde-Clarke's significant research concerning the *urban* digital divide, which includes a comparative analysis of Internet cafés in Johannesburg (Hyde-Clarke 2006), Prem Subramony's innovative study regarding the digital divide in the Alaskan Arctic (Prem Subramony 2007) and the essay by Martin and Robinson regarding the main social aspects of the digital divide (Martin and Robinson 2007).

difficult to reach, or the recent case of Congo[18]). Cuba, as we will see,[19] is a case unto itself: submarine cables belonging to nations in commercial and political conflict[20] with Cuba have run alongside the island for years, if not decades, but only in 2011 were there any concrete moves toward creating an efficient cable system. In these regions either the use of Internet is nearly unknown, or is known only to small groups of government functionaries and diplomats and in tourist facilities.

There are, then, other nations which, while possessing modern technological infrastructure, purposely aim to keep their populations *away* from the Internet, and do so by elevating associated costs or by requiring bureaucratic procedures so onerous as to render the process nearly impossible (Cuba is a clear example of this: the few and costly satellite connections have generally been available for use only by government functionaries), or a government may seek to limit as much as possible online actions once an Internet user finally does manage to go online, keeping their citizens under close watch whenever they go online (this is the situation in countries such as China,[21] Egypt[22] and Tunisia,[23] among others, which invest simultaneously in technology *tout court* and in technology to *control the use* of any technology made available to citizens).

Regarding this issue, those studies that highlight the correlation between the diffusion of the media in a given country, the manifestation of the digital divide, and the power and reach of control by authorities, are of significant interest.

Guillén and Suárez outline this aspect very well (Guillén and Suárez 2005), basing their considerations on the premise that *democratic* political regimes enable a *faster growth* of the Internet than *authoritarian* or *totalitarian* regimes. According to these scholars, media that enable decentralized mass communication undermine the effectiveness of authoritarian or totalitarian rules by allowing citizens to secure their own information, as opposed to that sponsored by the regime, and to communicate with one another and, potentially, to mobilize politically.

These two types of media pose a threat to the monopoly of information production, storage, dissemination, and communication that authoritarian and totalitarian regimes seek to establish and maintain.

As Guillén and Suárez so insightfully describe, the greater civil liberties of democracy are consistent with greater access to (and use of) the Internet, since gov-

[18] *BBC News* announced, in June 2012, that remote rural communities of Congo may soon have mobile coverage thanks to an International collaboration between Pan-African telecom provider RascomStar-QAF, Viasat and UK-based ip.access plan. The aim is to use small cells (called "picocells") to ensure coverage in the Congo's rainforest and to install 50 mini base stations around Congo. Each cell will then create a private wireless network in a particular area. (BBC 2012).

[19] See Sect. 6.2.2.

[20] An interesting essay by Fitzgerald explains the history of the United States trade policy on blacklisting and boycotts and the extraterritorial application of United States economic sanctions and trade controls, especially focusing on Cuba (Fitzgerald 1998).

[21] See Sect. 6.2.7.

[22] See Sect. 6.3.1.

[23] See Sect. 6.3.2.

ernments find it more difficult to censor free expression on the Internet than on television (Guillén and Suárez 2005). The consequence is that, in an age of electronic communication, totalitarian or authoritarian regimes find it more difficult to control information, communication, dissidents, and the press. Thus, in attempting to secure their stability and survival, authoritarian and totalitarian regimes regulate the use of the Internet in a variety of ways that are detrimental to its use.

According to these two authors, governmental efforts to control the Internet may include some, or all, of the following:

1. restricting access by controlling networks and instituting registration requirements (Guillén and Suárez 2005: 687–688);
2. restricting content by filtering information, blocking forbidden sites, taking disciplinary actions, and even making virus attacks on banned sites (Guillén and Suárez 2005: 687–688); and
3. credibly threatening to arrest or imprison those who access unauthorized information or use the Internet to organize and mobilize politically (Guillén and Suárez 2005: 687–688).

In the most extreme cases, the authoritarian or totalitarian government directly controls all *physical access* to the Internet (Guillén and Suárez 2005: 687–688).

Thus this first, geographical "difficulty", based on the enormous divergence of the availability and quality of technology in the various regions of the world, forces anyone seeking greater understanding of this issue to study the matter region by region and, in some cases, country by country.

Precisely to that end, many organizations whose work is to monitor the levels of digital liberty worldwide (for example: the *OpenNet Initiative*[24]) send their observers to the various nations of the world in order to gain a "field view" of local situations (including attempts to connect to foreign or blocked web sites and visits to Internet cafés to verify levels of government mandated surveillance and monitoring).

An interesting 2008 cablegram, recently released by *WikiLeaks*, written by an American government functionary in Cuba (the title of the document[25] is, significantly, *Surfing the Net in Havana*) clearly illustrates not only this type of local analysis, but also its importance in terms of how to technically circumvent certain restrictions.

The text of the cablogram explains several limitations, and in particular:

1. it is extremely difficult, if not impossible, to change the browser from *Google.cu* to *Google.com*, to *Google.ch* (Switzerland) or even to *Google.cr* (China);
2. it is difficult to access the web pages of some "critical" web sites, such as *Directorio Democratico Cubano*, the *Cuba Center for a Free Cuba*, or the *Grupo de Apoyo a la Disidencia*;

[24] In Internet at the address http://opennet.net/. Accessed 10 October 2011.

[25] See the complete text of the cablegram at the address http://cablesearch.org/cable/view.php?id=08HAVANA660&hl=farrar+net+havana. Accessed 10 October 2011. See, also, 6.2.2.

3. if the *Google.cu* browser is set on the "Cuba pages" option, the results of *Google* searches are strikingly different from a search activity done using *Google.com*.

The diplomat's final suggestion was, for the American government, to keep close watch of the evolving local Internet conditions in Cuba, and to seek to provide programs that would allow Cubans to circumvent Internet filters.

Therefore, two principal factors, *geography* and *digital divide*, create such enormous differences worldwide that it is quite clear that any useful examination of regions considered would, due to the very nature of the subject at hand, also include an in-depth analyses of the principal political and social frameworks as well. The last portion of this book, consequently, seeks to provide a clear and concise description of several regions worldwide, with additional emphasis placed on those nations where critical conditions exist.

Above all, we will describe how digital dissidents carry out opposition activities in their respective home countries (and what techniques and technologies they use), the legal frameworks employed by their governments to limit the free speech and, in the most serious cases, the human and civil rights of their citizens, and, finally, how these scenarios are changing.

In particular, there are two legal scenarios that are emblematic of the contexts in which many digital dissidents operate:

1. nations which have a legal apparatus that is in clear violation of basic fundamental human rights;
2. nations which apparently, or perhaps only formally, are more respectful of human rights and free speech (for example: nations that have adhered to Conventions regulating these matters,[26] or that have included in their Constitutions articles aiming to protect certain individual rights) but that in reality, within their borders, more or less systematically operate in violation of these rights (for example: permitting the broadest interpretation and application of the provisions of repressive laws).

Despite these considerable geographical, technological and legal diversities, it should be noted that there are also a number of constants with regard to the international response to digital dissidence, to which we will return repeatedly throughout this study, given that they are extremely significant.

The first is that the legal "strategies" or "excuses" utilized by a majority of nations to control technology and the activists and dissidents who use it, are surprisingly similar in every part of the world.

[26] We refer in particular to: the 1948 *American Declaration of the Rights and Duties of Man*; the 1948 *Universal Declaration of Human Rights* (UDHR); the 1950 *Convention for the Protection of Human Rights and Fundamental Freedoms*, commonly known as the *European Convention on Human Rights (ECHR)*; the 1966 *International Covenant on Economic, Social and Cultural Rights* (ICESCR); the 1966 *International Covenant on Civil and Political Rights* (ICCPR); the 1981 *African Charter on Human and Peoples' Rights*; the 1982 *Declaration on the Freedom of Expression and Information* of the Committee of the Ministers of the Council of Europe; the 1999 *United Nations Convention on the Rights of the Child* (CRC); the 2007 *Convention on the Rights of Persons with Disabilities*.

To briefly introduce them, they might be outlined as follows:

(a) laws regulating the press and other media whose application is extended to the digital world, often thanks to a strained, or even purely, artificial interpretation, which thus may lead to the sanctioning, or even incarceration, of bloggers, to accusations of "clandestine press", to difficulties in operating independent newspapers, to the revocation of "journalism licenses", to foreign travel restrictions and bans for bloggers, journalists and, sometimes, even students;
(b) legislation mandating registration for journalists, newspapers and blogs,[27] or the obligation to join certain associations solely for the objective of establishing greater control over not only any political views expressed, but also over *content* in general. This method is quite useful in inducing the practice of *self-censorship*,[28] and is quite diffused: even in apparently free legal contexts, the fact that journalists are "identified" and forced (and even when they are only "encouraged") to operate within a determined political framework, clearly leads to a perception of being under control, and results in an atmosphere in which many would rather not pursue certain news items for fear of retaliation. Thus they self-censor themselves, because they feel that they are institutionally controlled and monitored, not dissimilar to those countries in which the press is constantly threatened by organized crime;
(c) an intensive recourse to the offence of *defamation*, present in criminal codes of nearly every nation, as an instrument to avoid criticism of the government and its functionaries, of important national or religious symbols, of the nation's history or its founders, or to avoid debate on religious issues. Often the use of new technologies in perpetrating an alleged defamation is considered an aggravating factor;
(d) The use of criminal law provisions to limit or prohibit demonstrations, assemblies, meetings and traditional forms of protest;

[27] See, *inter alia*, Uzbekistan's 2007 *Media Law*, amended in 2010 to oblige web sites to register and to provide information on their employees and copies of their articles to the government (see Sect. 6.2.9.2). See, also, the similar legal framework in Iran, with the *Press Law* of 1996 (see Sect. 6.2.6).

[28] On the topic of self-censorship see, *inter alia*, the enlightening study by Hayes, Scheufele and Huge on *non participation as self-censorship* in a different political framework (Hayes et al. 2006) and on the concern that, in a polarized opinion climate, people may refrain from participating in publicly observable political activities that make them vulnerable to *scrutiny* and *criticism* by others who hold opinions that differ from their own (Hayes et al. 2006: 259). The authors explained also that in a polarized, hostile political climate, some people decide not to participate in public forms of opinion expression because there may be *negative social ramifications* of doing so: "when we let other people know what we think, we set ourselves up for scrutiny, criticism, and perhaps even social ostracism" (Hayes et al. 2006: 263–264).

(e) The use of special laws to impede communication both *toward* foreign countries (media monitoring and blocks, Internet shut-down[29]) especially during political upheaval, or around certain anniversaries, which run the risk of degenerating into violence, as well as *from* foreign countries (ranging from extreme measures such as prohibiting all satellite receivers and connection boxes, to "merely" monitoring all Internet cafés connections and resorting to intense Internet filtering programs);
(f) The use of laws which prohibit and sanction collaboration with enemy nations, protect the integrity and the independence of the state, its sovereignty, state and other official secrets, and which prohibit the diffusion of classified documents.

In this type of legal environment, individuals who resist, who dare to rebel and to speak out, have developed ways and techniques to *circumvent* certain restrictions which, however, are also extremely dependent upon the state of the nation in which they live and specifically upon its technological development.

As we will explain, one of the most interesting elements of digital resistance movements currently taking place around the globe is the myriad ways in which available, and even obsolete, technology is adapted, sometimes ingeniously, to the needs of the dissidents and activists who use it.[30]

Thus the first difficulty facing researchers, based on diverse geographical realities, leads to a second one, related to vastly *differing legal environments*.

It is well-known that, for many years, international legal bodies, seeking to guarantee uniformity in the level of protection of human rights, have attempted to regulate these matters by Declarations, Conventions and Treaties, more recently applying these general principles to the digital world as well.

However, a global investigation of these rights, such as that forming the central portion of the present analysis,[31] reveals with startling clarity that the formal adhesion by certain nations to the principals of human rights is unfortunately not always correlated to consequent levels of liberty and to the respect of those human rights in concrete terms within national borders.

In fact, it can be much more interesting for the legal observer of such matters, to analyze those episodes of violation of human rights or attempts at censorship in precisely those countries that claim maximum respect for human rights and that have adhered to numerous Conventions and Treaties, rather than similar episodes in nations that are already notorious for such behavior.

---

[29] For example, the Internet shut-down in Burma during the widely followed protests led by Buddhist monks in 2007 (see Sect. 6.2.1), and, prior to that, the martial law declared by the King in Nepal in 2005 with the shut-down of Internet connections and mobile phones lines. See, also, the Internet shut-down in Egypt in 2011 (see Sect 6.3.1). Goldstein and Rotich also cite an episode of tentative SMS shut-down in Kenya: as messages of hate extended their reach into the Kenyan population, Michael Joseph, the CEO of *Safaricom*, Kenya's largest mobile phone provider, was approached, the scholars write, by a government official who was considering shutting down the SMS system. Goldstein and Rotich write that Joseph convinced the government not to shut down the SMS system, and instead to allow SMS providers to send out messages of peace and calm, which *Safaricom* did to all nine million of its customers (Goldstein and Rotich 2008: 5).

[30] See Chap. 5.

[31] See Chap. 4.

Attempts at covert censorship, and at laws and bills seeking to limit free speech in countries that are, from a legal point of view, advanced, are often among the most dangerous. With reference, then, to Internet liberties and to the over-protection of intellectual property rights which has resulted in the clear overshadowing of the right to the free circulation of knowledge and culture, the present work has also examined, incidentally, countries such as Italy[32] or the United States of America, all of which have repeatedly faced censure with regard to these and similar issues.

The third interpretative challenge facing the legal scholar is how to connect the phenomena of rebellion and dissidence to the *noble tradition of hacking*, which gave rise to, and has shaped, the history of the computer age from its very beginnings in the 1950s and which, over the course of the last six decades, has gradually lost its association with play, innocent openness and curiosity and has gained a modern, and in most cases completely unjustified, connotation of criminal behavior.

The words with which Levy opened his famous book *Hackers – Heroes of the Computer Revolution* are significant in describing the essence of this movement and in providing a more accurate definition of hackers (Levy 1984). Levy addresses *seven key points*, and in particular, according to his interpretation, hackers are:

1. *computer lovers*. Hackers, from the scholar's point of view, are those computer programmers and designers who regard computing as the most important thing in the world (Levy 1984: 4);
2. *non standard people*. Hackers are not nerdy social outcasts or "unprofessional" programmers who write dirty, "nonstandard" computer code, but, quite to the contrary, are truly fascinating individuals (Levy 1984: 4);
3. *revolutionaries*. Hackers are adventurers, visionaries, risk-takers, artists, and the ones who most clearly saw why the computer was a truly revolutionary tool (Levy 1984: 4);
4. *multifaceted*. Hackers range from those who tamed multimillion-dollar machines in the 1950s to contemporary young wizards who mastered computers in their suburban bedrooms (Levy 1984: 4);
5. *tinkers*. Hackers have a common element, a common philosophy which seemed tied to the elegantly flowing logic of the computer itself, a philosophy of sharing, openness, decentralization, and getting hands on machines at any cost to improve the machines, and to improve the world (Levy 1984: 4);
6. *ethichals*. The hacker ethic is their gift to humanity, and is embodied in the behavior of hackers themselves (Levy 1984: 4);
7. *etherogeneous*. The hacker's genus include the true hackers of the MIT *Artificial Intelligence Laboratory* in the 1950s and 1960s, the populist, less sequestered hardware hackers in California in the 1970s, and the young game hackers who made their mark in the personal computer age of the 1980s (Levy 1984: 4).

[32] For a general introduction to the regulatory framework of cyberspace law in Italy, see Ziccardi 2011.

It is widely known that some dissidents are also computer geniuses, and have no qualms about "hacking the system" for their political aims. It is equally well known that the majority of cultural movements rotating around the hacking world look kindly upon this type of activity (including that of sites similar to *WikiLeaks*, which seek to increase transparency) and often, from their own countries of residence, seek to assist.

And it is, also, well known that hackers' constant monitoring of the so-called "state technologies", those technologies used by governments to monitor, to filter and to render their own actions less transparent and more closed off from the sight and judgment of their own citizens, is in all likelihood positive for today's society.

It is also true, however, that the current hacking environment is much more complex than it was even 20 years ago, due both to the ease with which it is now possible to perform certain actions, by simply automatizing them, and to the fact that a number of nations have created veritable hacker training schools, preparing young computer prodigies to embark upon cyber-wars, with evident problems in terms of the ethical use of technology.

This study seeks to address, from a perspective that is at the same time technical and legal, the following three issues:

1. worldwide digital resistance and dissidence, both interpreted in the widest sense, with an in-depth look at the current situations in a few of the most critical countries;
2. the techniques used locally for digital resistance; and,
3. the relationships between hacking, the open data movement, leaking and whistle-blowing issues and the transparency of information.[33]

It is hoped that this type of analysis will aid the reader in navigating through the recent debates[34] surrounding the idea that technologies (e.g. *Twitter* and *Facebook*) can lead to revolutions, with technology seen, in this view, as the essential motor for the political upheavals of the last 10 years, or whether, to the contrary, technology has played only a marginal role, and has, in fact, often been more instrumental in repressing, rather than facilitating, change.

As the scholar Morozov states, perhaps there should be less enthusiasm and more attention in bringing a proper analysis of the political impact and the power of new technologies in current political landscapes, but, of course, this it is not a matter of little importance in this context. Morozov remarks that the Internet, *Facebook* and *Twitter* do not have *magical qualities* that can *automatically* open up

[33] See Aron's overview of digital conflicts and *real life* (Aron 2010) and Papandrea's remarks on the publication of *national security information* in the digital age (Papandrea 2011),

[34] For a first, qualified idea of this debate, see, *inter alia*, the studies of Beutz Land on networked activism (Beutz Land 2009), of Morozov on the revolution in Iran (Morozov 2009), of Comninos on cyber crackdowns (Comninos 2011), of Liste Muñoz and de Soysa on political repression in the digital era (Liste Muñoz and de Soysa 2011), of Hatem Ali on the power of social media in critical contexts (Hatem Ali 2011) and of Hashemi-Najafabadi on information revolution in Muslim societies (Hashemi-Najafabadi 2010).

closed societies and repressive or authoritarian regimes (Morozov 2011: XII). As another mindful scholar of these topics, Zuckerman, recently observed, it is wrong, in fact, to try to credit *a single factor* (technological, economical or political) for these revolutions, but the role of online media is, without a doubt, highly significant. Tunisians, Zuckerman observes, took to the streets due to decades of frustration, not in reaction to a *WikiLeaks* cable, a denial-of-service attack, or a *Facebook* update.[35] However, it is certainly clear that online media did play a role in helping Tunisians learn about the actions their fellow citizens were taking, and in making the decision to *mobilize* (Zuckerman 2011).

I, personally, do not believe that revolutions and epochal change can be brought about *solely* by technology, however advances it may be. At the end, the actions, strategies, and choices are always made by humans. But, at the same time, it is also true that, over the years, technology has demonstrated its enormous potential for changing the lives of mankind; thus, with regard to the importance of technology, it is necessary to carefully evaluate every event, and only then to decide how, and how much, technology has, in that context, facilitated or hindered activists and their work.

Certain truths, however, are undeniable: today technology is the most powerful means ever seen to diffuse information, to circumvent even formidable state filtering, and monitoring systems, to find, in real time, other people who share similar ideas and who, perhaps, plan to act and protest. Technology can add velocity to simple thoughts and plans, speeding them toward fruition, the velocity that comes from knowing that only a few hundred kilometers, or a few thousand kilometers away, there are others who think the way we do, and who are also ready to act.

Technology may not "create" revolutions, but it is also true that, without technology, the majority of the revolutions of recent years would have, in all likelihood, had far greater difficulty in igniting the spark that propelled them toward history.

An illuminating study by Wheeler on how the Internet has changed the lives of common Internet cafés users in Jordan and Egypt (Wheeler 2006), conducted in 2004, and drawing on interviews with more than 200 users, is very significant in that it was one of the first to provide a clear description of the *impact* that the network had, over the first decade of Internet diffusion in those countries, among different layers of the population.

The study deals with non-professional users without Internet connections at home, who visited web sites and forums from public access stations. In the Arab world, Internet arrived gradually, at the beginning of the 1990s: Tunisia was the first Arab state to connect to the Internet in 1991, followed by Kuwait in 1992 and Egypt, Turkey and the UAE in 1994, while Syria and Saudi Arabia were the last, with regular access from the late 1990s (Wheeler 2006: 6).

An interesting factor is described in Wheeler's study: even then, many users tended to learn the use of the Internet within the Internet cafés, and were either *self-taught* or learnt through the *explanations* of relatives or friends (Wheeler 2006: 9).

[35] See Sect. 6.3.2.

Access to the Internet allowed users to improve their English language skills, to broaden their visions (including in terms of politics) and to create social and professional networks; another important novelty was the possibility for women to converse with men (Wheeler 2006: 12). The Internet, Wheeler writes, permitted decades of segregation to be overcome, and allowed the exchange of ideas between genders, along with a gradual mental openness and a less conservative approach (Wheeler 2006: 12). The advent of the web in those countries allowed not only international borders, but also the numerous geographic and cultural barriers existing within those countries, to be overcome (Wheeler 2006: 12). Women began to speak in public places, although they were virtual spaces, and to do this even "in front" of men (Wheeler 2006: 12).

These technologies began to help people to gain access to restricted information and to form a *political consciousness*, where policy can be intended as a place for discussion and comparison of different ideas, and get to know people outside of the typical, common, usual circle, permitting a further openness (Wheeler 2006: 12). People became more informed, more information brought greater security in expressing opinions or led people to expose themselves more (Wheeler 2006: 12). At the same time, this new consciousness increased the level of education and the level of understanding of events, leading to the creation of a so-called public sphere[36] (Wheeler 2006: 14, 18).

Two very important activities in this public sphere are those that became so important during the social and political movements that have now come to be called the *Arabian Spring*, i.e. *activism* and *blogging*.

Wael Ghonim notes several important points regarding the *Arabian Spring* and the so-called *blogosphere* (Khoury 2011: 80):

1. *collective contribution of content*. He describes the events, in Egypt, as a sort of *Revolution 2.0*, where everyone contributed content, small pieces of information and bits of knowledge and debate, without knowing the names of the other people contributing the content as well (Khoury 2011: 80–83);
2. *political power of the blogosphere*. The Arab world has certainly witnessed a mushrooming of the blogosphere and digital activism over the past few years, and political blogging has been hailed by many as a *major force* and *vehicle* for change and reform in the region (Khoury 2011: 80–83);
3. *reaction to censorship*. The Arab blogosphere arose because young people were frustrated with the *restrictions* imposed by the state regulated boundaries of the Arab public sphere, which was closed off to most modes of free expression and joint citizen action (Khoury 2011: 80–83);

[36] For the concept of *public sphere* see the studies by Habermas (Habermas 1964). The public sphere is "[…] first of all a realm of our social life in which something approaching public opinion can be formed. Access is guaranteed to all citizens. A portion of the public sphere comes into being in every conversation in which private individuals assemble to form a public body. […] Citizens behave as a public body when they confer in an unrestricted fashion that is, with the guarantee of freedom of assembly and association and the freedom to express and publish their opinions about matters of general interest" (Habermas 1964: 49). See, also, Sect. 2.1.3.

4. *creation of a new virtual public sphere*. Advances in new mass communication technologies that have revolutionized expression and collapsed boundaries between people (both within and across countries), have allowed young Arabs to relocate civic action and expression from the suffocated (physical) public sphere to the Internet, and in so doing, they have created a *new virtual public sphere* (Khoury 2011: 80–83);
5. *bloggers violent repression*. The political significance of blogging and social media as a whole is evidenced by the fact that, in recent years, Arab regimes have cracked down on bloggers with increasing rigor and ferocity. Although this crackdown was most visible in Egypt, which has one of the largest and most dynamic of the region's blogospheres, other countries such as Morocco and Syria, have also detained and jailed bloggers for online activism (Khoury 2011: 80–83);
6. *use of the technology for the purpose of witnessing*. Bloggers and online activists have amassed a different and more subtle kind of power. Advances in video and photography technology have not only made digital cameras and video recorders accessible to lay people, but have allowed online activists to document, photograph and record human rights violations, government negligence, police violence and other incidents of daily life, and share them with the vast online community. Once this information is online, it is impossible to eliminate or stop it from spreading (Khoury 2011: 80–83);
7. *Internet as an organizing tool*. Many activists were introduced to activism and incorporated into activist groups by first making contact on the web. The Internet was a medium of theorizing, campaigning and organizing. All in all, it was a method of *activating* the community (Khoury 2011: 80–83).

An interesting study by Hashemi-Najafabadi concerns the creation, after the information revolution, of the afore mentioned *new public sphere* in Muslim societies (Hashemi-Najafabadi 2010). A first interesting point, for the scholar, is that the information revolution has contributed to the *fragmentation of authority* in the Muslim world, especially regarding the *print industry*, which initially helped the religious authority to monopolize religious publications and to *control religious discourse*. Nevertheless, the increasing number of educated people who had access to the Islamic classics in their own vernacular languages undermined the authority of *ulama* (traditional religious scholars), who thus began to lose their "monopoly of the transmission of knowledge", and Internet played a major role in spreading knowledge in this society (Hashemi-Najafabadi 2010: 4). A second point is defined, by the author, as the *trust competition:* since the advent of the mass media by the invention of radio, television and especially satellite television, as well as the spread of newspapers in wider scenes, different voices have been competing to reach and to motivate more and more audiences (Hashemi-Najafabadi 2010: 4).

The two final statements of the scholar are as follows:

1. that period was a time when *public* and *private* were distinguishable, but today, *Web 2.0* tools "bypass many of the barriers to visibility found in the established media" and act as watchdogs (Hashemi-Najafabadi 2010: 13);

2. in this sense, since it is too difficult to censor new media and control how information is disseminated through them, the states no longer can feel free to do whatever they desire without being accused by public opinions. This was exactly what happened during the recent political crisis in Iran. A few years ago, it was easy for the state to keep even important incidents completely secret, whereas today, a single young woman dies in a street in Tehran, and millions of people immediately read and even *watch* the story on blogs, *Facebook* or *YouTube*, make comments on the event and organize protests (Hashemi-Najafabadi 2010: 13).

Also quite interesting, regarding these issues, is the story of *Nawaat.org*, an independent collective blog on Tunisia,[37] originally launched in order to provide a public platform for oppressed voices and debates; today, it provides information on the Tunisian revolution, culture, socio-economic and political developments, corruption, governance and issues of censorship. This Tunisian blogging collective won, in 2011, the prestigious *EFF Pioneer Award* because it played a crucial role in covering the social and political unrest in Tunisia which ended in the toppling of Ben Ali's regime. EFF stated that the prize went to *Nawaat* because it "disseminated day-by-day user-generated news about the uprising, and helped bridge the gap between international mainstream media and citizen journalists and activists by aggregating and contextualizing information spread through social media".[38]

Concerning the importance of social media in Egypt, Zhuo, Wellman and Yu outline three fundamental aspects:

1. it is clear that social media such as *Facebook* played important roles in transforming organized groups and informal networks, establishing external linkages, developing a sense of modernity and community, and drawing global attention to diverse issues and events that might otherwise have gone unnoticed (Zhuo et al. 2011: 6, 9);
2. their impact suggests that those concerned with the quest for democracy and peace should pay more attention to the explicit and implicit effects of these social media (Zhuo et al. 2011: 6, 9);
3. the ways in which the revolt played out more subtly suggest that, much like Western societies, parts of Egyptian society are transforming away from traditional groups and towards more loosely structured "networked individualism." There is less group control – and more autonomy – in networked societies (Zhuo et al. 2011: 6, 9).

In Egypt, Zhuo, Wellman and Yu remark the manifestation of a *triple revolution* of the type that has already occurred in Western societies. The three aspects of this type of revolution are:

1. the turn to social networks (Zhuo et al. 2011: 6, 9);
2. the proliferation of the far-flung, instantaneous Internet (Zhuo et al. 2011: 6, 9);

[37] In Internet at the address http://nawaat.org/portail/. Accessed 15 November 2011.

[38] See the EFF press release regarding the *Pioneer Award* at the address https://www.eff.org/press/releases/us-senator-encryption-innovator-and-tunisian-blogging-group-win-eff-pioneer-awards. Accessed 23 November 2011.

3. the even wider proliferation of constantly available mobile phones (Zhuo et al. 2011: 6, 9).

These scholars close their fascinating article with three final statements, which they framed within the specific context of Egypt, but which may also be extended to the giddy events that are occurring in schools and offices, backstreets and central plazas, Internet cafés and government buildings, and in simple homes in diverse regions throughout the world:

1. *the importance of the people*. The success of the revolt should be credited to Egyptian people (Zhuo et al. 2011: 6, 9); but, at the same time,
2. *the undeniable importance and impact of social media*. The impact of social media should not be overestimated but is *undeniable* that social media played an important role in the *mobilization* and *organization* of the Egyptian revolt (Zhuo et al. 2011: 6, 9);
3. *the birth of a revolutionary community*. Social media role intertwined with the development of formal organizations, informal networks and external linkages, fosters a growing sense of modernity and community, and globalizes support for the revolt (Zhuo et al. 2011: 6, 9).

References

Aron, Jacob. 2010. WikiLeaks wars: Digital conflict spills into real life. http://www.newscientist.com/article/mg20827913.400-wikileaks-wars-digital-conflict-spills-into-real-life.html. Accessed 6 Nov 2011.

Attewell, Paul. 2001. The first and second digital divides. *Sociology of Education* 74(3): 252–259.

Bannister, Frank, and Regina Connolly. 2010. The trouble with transparency: A critical view of openness in e-government. http://microsites.oii.ox.ac.uk/ipp2010/system/files/IPP2010_Bannister_Connolly_Paper.pdf. Accessed 6 Nov 2011.

BBC. 2012. Remote parts of Congo may soon get mobile coverage. 5 June 2012. http://www.bbc.com/news/technology-18333727. Accessed 11 June 2012.

Beutz Land, Molly. 2009. Networked activism. *Harvard Human Rights Journal* 22: 205–243. http://harvardhrj.com/wp-content/uploads/2009/09/land.pdf. Accessed 14 Nov 2011.

Comninos, Alex. 2011.Twitter revolutions and cyber crackdowns – User-generated content and social networking in the Arab spring and beyond. http://www.apc.org/en/system/files/AlexComninos_MobileInternet.pdf. Accessed 22 Oct 2011.

De Roy Olivier, Coeur. 1997. The African challenge: Internet, networking and connectivity activities in a developing environment. *Third World Quarterly* 18(5): 883–898.

Diamond, Larry. 2010. Liberation technology. *Journal of Democracy* 21: 69–83.

Ensemble, Critical Art. 1995. *Electronic civil disobedience: And other unpopular ideas*. New York: Autonomedia.

Ensemble, Critical Art. 2000. Recombinant theatre and digital resistance. *TDR* 44(4): 151–166.

Ensemble, Critical Art. 2001. *Digital resistance: Explorations in tactical media*. New York: Autonomedia.

Etling, Bruce, Robert Faris, and John Palfrey. 2010. Political change in the digital age: The fragility and promise of online organizing. http://dash.harvard.edu/handle/1/4609956. Accessed 14 Nov 2011.

Fitzgerald, Peter L. 1998. Pierre goes online. Blacklisting and secondary Boycotts in U.S. Trade policy. *Vanderbilt Journal of Transnational Law* 31: 1–96.

Freiberger, Paul, and Michael Swaine. 2000. *Fire in the valley: The making of the personal computer*. New York: McGraw-Hill.

Goldstein, Joshua, and Juliana Rotich. 2008. Digitally networked technology in Kenya's 2007–2008 post-election crisis. http://cyber.law.harvard.edu/sites/cyber.law.harvard.edu/files/Goldstein&Rotich_Digitally_Networked_Technology_Kenyas_Crisis.pdf.pdf. Accessed 13 Nov 2011.

Graham, Mark. 2011. Time machines and virtual portals. The spatialities of the digital divide. *Progress in Development Studies* 11(3): 211–227.

Guillén, Mauro F., and Sandra L. Suárez. 2005. Explaining the global digital divide: Economic, political and sociological drivers of cross-national internet use. *Social Forces* 84(2): 681–708.

Habermas, Jürgen. 1964. The public sphere: An encyclopedia article (1964). *New German Critique* 3: 49–55.

Hands, Joss. 2001. *@ is for activism: Dissent, resistance and rebellion in a digital culture*. London: Pluto Press.

Hashemi-Najafabadi, S.Adel. 2010. Has the information revolution in Muslim societies created new publics? *Muslim World Journal of Human Rights* 7(1). doi:doi:10.2202/1554-4419.1187.

Hatem Ali, Amir. 2011. The power of social media in developing nations: New tools for closing the global digital divide and beyond. *Harvard Human Rights Journal* 24: 185–219. http://www.mobileactive.org/files/file_uploads/185-220.pdf. Accessed 14 Nov 2011.

Hauben, Michael. 1996. Participatory democracy from the 1960s and SDS into the future on-line. http://opencollector.org/history/homebrew/netdemocracy-60s.html. Accessed 10 Oct 2011.

Hayes, Andrew F., Dietram A. Scheufele, and Michael E. Huge. 2006. Nonparticipation as self-censorship: Publicly observable political activity in a polarized opinion climate. *Political Behavior* 28(3): 259–283.

Heinzelman, J., R. Brown, and P. Meier. 2011. Mobile technology, crowdsourcing and peace mapping: New theory and applications for conflict management. In *Mobile technologies for conflict management. Online dispute resolution, governance, participation*, ed. Marta Poblet, 39–53. Dordrecht, Heidelberg, London, New York: Springer.

Hyde-Clarke, N. 2006. The urban digital divide: A comparative analysis of internet cafés in Johannesburg, South Africa. *Review of African Political Economy* 33(107): 150–156.

Khoury, Doreen. 2011. Social media and the revolutions: How the internet revived the Arab public sphere and digitalized activism. In people's power – the Arab world in revolt. Perspectives special issue 80–85. http://www.lb.boell.org/downloads/02_Perspectives_ME_2011_The_Arab_World_in_Revolt.pdf. Accessed 10 Nov 2011.

Klang, Mathias. 2004. Civil disobedience online. *Journal of Information, Communication and Ethics in Society* 2: 75–83.

Korenblum, J., and B. Andemariam. 2011. Cell phones and conflict zones: How souktel uses SMS technology to empower and aid in conflict-affected communities. In *Mobile technologies for conflict management. Online dispute resolution, governance, participation*, ed. Marta Poblet, 67–78. Dordrecht, Heidelberg, London, New York: Springer.

Lash, Bob. 2006. Memoir of a homebrew computer club member. http://www.bambi.net/bob/homebrew.html. Accessed 10 Oct 2011.

Lessig, Lawrence. 2009. Against transparency. The perils of openness in government. http://www.tnr.com/article/books-and-arts/against-transparency. Accessed 6 Nov 2011.

Levy, Steven. 1984. *Hackers – Heroes of the computer revolution*. New York: Delta Book.

Liste Muñoz, Lucia, and Indra de Soysa. 2011. The blog versus big brother: New and old information technology and political repression, 1980–2006. *The International Journal of Human Rights* 8: 1315–1330.

Livingston, Jessica. 2007. *Founders at work: Stories of startups' early days*. New York: Apress.

Martin, Steven P., and John P. Robinson. 2007. The income digital divide: Trends and predictions for levels of internet. *Social Problems* 54(1): 1–22.

Miard, Fabien. 2009. Mobile phones as a tool for civil resistance. Case studies from Serbia and Belarus. http://www.digiactive.org/wp-content/uploads/research3_miard.pdf. Accessed 22 Oct 2011.

Morozov, Evgeny. 2009. Iran: Downside to the "Twitter Revolution". *Dissent* 56(4): 10–14.
Morozov, Evgeny. 2011. *The net delusion: The dark side of internet freedom*. New York: PublicAffairs.
Natriello, Gary. 2001. Bridging the second digital divide: What can sociologists of education contribute? *Sociology of Education* 74(3): 260–265.
Papandrea, Mary-Rose. 2011. The publication of national security information in the digital age. *Journal of National Security Law & Policy* 5: 119–130. http://www.jnslp.com/wp-content/uploads/2011/06/03_Papandrea.pdf. Accessed 7 Nov 2011.
Pattaro, Enrico, and Giovanni Sartor. 2002. Norms, laws and the internet. http://www.ieid.org/congreso/ponencias/sartorpattaro.pdf. Accessed 14 Nov 2011.
Peckham, Michael. 1998. New dimensions of social movement/countermovement interaction: The case of scientology and its internet critics. *The Canadian Journal of Sociology* 23(4): 317–347.
Pfaffenberger, Bryan. 1988. The social meaning of the personal computer: Or, why the personal computer revolution was no revolution. *Anthropological Quarterly* 61(1): 39–47.
Prem Subramony, Deepak. 2007. Understanding the complex dimensions of the digital divide: Lessons learned in the Alaskan Arctic. *The Journal of Negro Education* 76(1): 57–67.
Radden Keefe, Patrick. 2005. *Chatter. Dispatches from the secret world of global eavesdropping*. New York: Random House.
Rosenzweig, Roy. 1998. Wizards, bureaucrats, warriors, and hackers: Writing the history of the internet. *The American Historical Review* 103(5): 1530–1552.
Russell, Adrienne. 2005. Editorial: Exploring digital resistance. *New Media & Society* 7: 513–515.
Salazar, O., and J. Soto. 2011. How to crowdsource election monitoring in 30 days: The Mexican experience. In *Mobile technologies for conflict management. Online dispute resolution, governance, participation*, ed. Marta Poblet, 55–66. Dordrecht, Heidelberg, London, New York: Springer.
Searle, John R. 1971. *The campus war: A sympathetic look at the University in Agony*. New York: World Pub. Co.
Sterling, Bruce. 1992. *The Hacker Crackdown – Law and disorder on the electronic frontier*. New York: Bantam.
Turner, Fred. 2005. Where the counterculture met the new economy. The WELL and the origins of virtual community. *Technology and Culture* 46(3): 485–512. http://www.stanford.edu/~fturner/Turner%20Tech%20&%20Culture%2046%203.pdf. Accessed 4 Nov 2011.
Turner, Fred. 2006. *From counterculture to cyberculture. Stewart Brand, the whole earth network, and the rise of digital utopianism*. Chicago: The University of Chicago Press.
Wagner, Todd H., M.Kate Bundorf, Sara J. Singer, and Laurence C. Baker. 2005. Free internet access, the digital divide, and health information. *Medical Care* 43(4): 415–420.
Wallsten, Scott. 2005. Regulation and internet use in developing countries. *Economic Development and Cultural Change* 53(2): 501–523.
Warf, Barney, and John Grimes. 1997. Counterhegemonic discourses and the internet. *Geographical Review* 87(2): 259–274.
Warschauer, Mark. 2003. Dissecting the "Digital Divide": A case study in Egypt. *The Information Society* 19(4): 297–304.
Wheeler, Deborah L. 2006. Empowering publics: Information technology and democratization in the Arab world – lessons from internet cafés and beyond. http://ssrn.com/abstract=1308527. Accessed 28 Oct 2011.
Whitty, Noel. 2010. Soldier photography of detainee abuse in Iraq: Digital technology, human rights and the death of Baha Mousa. *Human Rights Law Review* 10(4): 689–714.
Wozniak, Steve. 1984. Homebrew and how the apple came to be. http://www.atariarchives.org/deli/homebrew_and_how_the_apple.php. Accessed 8 Oct 2011.
Wray, Stefan. 1998. On electronic civil disobedience. http://www.thing.net/~rdom/ecd/oecd.html. Accessed 21 Oct 2011.

Zhuo, Xiaolin, Barry Wellman, and Justine Yu. 2011. Egypt: The first internet revolt? *International Journal of Emerging Technologies and Society* 8(1): 24–41. http://homes.chass.utoronto.ca/~wellman/publications/egypt/PMag-1107-Egypt-offprint.pdf. Accessed 21 Nov 2011.

Ziccardi, Giovanni. 2011. *Cyber law in Italy*. Alphen aan den Rijn: Kluwer Law International.

Zuckerman, Ethan. 2011. The first twitter revolution? Not so fast. The internet can take some credit for toppling Tunisia's government, but not all of it. *Foreign Policy* January 14, 2001. http://www.foreignpolicy.com/articles/2011/01/14/the_first_twitter_revolution. Accessed 4 Oct 2011.

Chapter 2
Digital Resistance, Digital Liberties and Digital Transparency

2.1 A Preliminary Definition of *Digital Resistance* and *Digital Liberties*

2.1.1 Some Focal Aspects of Digital Dissidence

Over the past decade, political and social events in several states have rendered issues such as digital resistance, liberation technologies, dissent, activism, hacking, hacktivism, radical transparency and open data not only the subject of animated discussions, but extremely topical as well.

The most important recent events are those that occurred in 2009 in Moldova,[1] in 2009–2010 in Iran,[2] in 2010–2011 in Tunisia[3] and in 2011 in Egypt[4] and Lybia.[5]

[1] For an understanding of the main issues regarding digital dissidence in Moldova see, *inter alia*, the studies by Morozov concerning the role of technology (Morozov 2009), Tismaneanu considerations regarding political and authoritarian issues (Tismaneanu 2009), Hodge's remarks from Moldova as events there were unfolding (Hodge 2009), the article by Mungiu-Pippidi and Munteanu on democracy issues in that context (Mungiu-Pippidi and Munteanu 2009), the study by Ciobanu regarding the future of Romania and Moldova (Ciobanu 2010) and the essay by Litra on the evolution of the multi-party system in that country (Litra 2010). Tismaneanu, in particular, believes that the people who took to the streets in Chisinau, and occupied the official buildings on National Assembly Square, are citizens who simply demanded the truth, who rejected hypocrisy and duplicity, and who refused to relinquish their human dignity in the face of abuse of power (Tismaneanu 2009).

[2] For an introductory framework on the Iran's *Green Revolution*, see Morozov on the main political and technological issues (Morozov 2009), Burns and Eltham regarding the evaluation of *Twitter*'s role in public diplomacy and information operations in Iran's 2009 election crisis (Burns and Eltham 2009), Sohrabi-Haghighat and Mansouri concerning ICT policy (Sohrabi-Haghighat and Mansouri 2010) and an interesting annotated bibliography on *Twitter* and the Iranian election protests edited by Forte (Forte 2009). Sohrabi-Haghighat and Mansouri outline how, in the absence of independent media, reports of the political upheaval were brought to the world by the protesters' extensive use of mobile phones and the Internet. The protesters, the authors recall, took advantage of information and communication technologies to disclose the regime's brutality by posting

G. Ziccardi, *Resistance, Liberation Technology and Human Rights in the Digital Age*, Law, Governance and Technology Series 7,
DOI 10.1007/978-94-007-5276-4_2, © Springer Netherlands 2013

As Morozov, for example, notes, referring to the events in Moldova, that the role of technologies was certainly thought-provoking. He outlines, in his preliminary analysis, three focal aspects:

1. *the important role of technology in similar hostile environments*. Morozov notes that technology played an important role in *facilitating protests*. In addition to huge mobilization efforts both on Twitter and Facebook, the scholar observes that Moldova's angry youth, especially those who were abroad (roughly a quarter of Moldova's population are working abroad due to dire economic conditions at home), followed the events on a livestream system provided by a Romanian TV station directly from the square. At the same time, there was little to no cellular phone coverage in the square itself (Morozov correctly observes that shutting down cellphone coverage in protest areas is a strategy that was also used by the Belarusian authorities during 2006 protests in Minsk), so protesters were forced to post updates to *Twitter* via GPRS technology on their mobile phones (Morozov 2009);
2. *the intense use of Twitter and blog posts*. Morozov observed, in those days of rebellion, that reports of the protests were posted on *Twitter* at record-breaking rates and blog posts were also being updated in real-time, minute by minute, in addition to the streaming of videos on *YouTube* and the diffusion of photos, including those uploaded to *Facebook* (Morozov 2009);
3. *mobilization and real time report of the protest*. Morozov's conclusion is that it would certainly be wrong to disregard the role that *Twitter* and other social media played in mobilizing (and, to an even greater degree, reporting on) the protests (Morozov 2009).

2.1.2 Preliminary Legal and Political Remarks

This phenomenon is extremely stimulating for legal scholars and observers of this brave new field

---

photos and video footage taken by mobile phones on the Internet, and, at the same time, the regime's measures failed to *control* the flow of news and information going out of the country (Sohrabi-Haghighat and Mansouri 2010: 24, 25). See, also, Sect. 6.2.6.

[3] For an introductory framework of Tunisia, see Ingram's essay concerning events in that country (Ingram 2011), the article by Zuckerman regarding the end of Tunisia's government (Zuckerman 2011) and the essay by Comninos on user-generated content and social networking during the *Arabian Spring* (Comninos 2011). See, also, Sect. 6.3.2.

[4] To understand the main issues regarding digital dissidence in Egypt, see, *inter alia*, the study by Hudson on the *Twitter*-revolution debate (Hudson 2011), the already cited article by Zhuo, Wellman and Yu on the first Internet revolt (Zhuo et al. 2010) and Abu El-Ata's study concerning technology issues during the Egyptian revolution (Abu El-Ata 2011). See, also, Sect. 6.3.1.

[5] To better understand the main issues regarding digital dissidence in Libya see, *inter alia*, Gheblawi's article on Libyan *re-independence* and revolution (Gheblawi 2011).

In fact, it would appear that the Internet, the electronic world, and personal computers have given rise to a new area of confrontation, albeit one with particular features.

There are a number of considerations that one might draw, not all of which, however, are wholly correct: is that the digital world, for those who wish to protest or to express their dissent, is *larger* (correct) and *more powerful* (this is also correct) but also *less dangerous* (incorrect, as we will see) and more likely *to allow user anonymity and* to *protect* those who use the Internet to act (this is also almost always incorrect, and the reader will also find evidence of this unfortunate reality).

The first two of the above points are not only true, but also interesting and quite novel: today technology is in the position to overcome boundaries, distribute data globally, such as news reports, video and audio clips, and, above all, allow dissidents to obtain aid and contributions from *outside* their areas of residence, which are often too repressive to allow safe operation (note that many digital protest events take place outside the country directly interested, as evidenced by fact that the redirected traffic and *Twitter* messages that divulge information about the events *from abroad* are often far more numerous than those originating in the country at the center of unrest or political upheavals). The three most common method of providing technological assistance to dissidents from abroad are (i) sending software intended to circumvent blocking or filtering systems, (ii) the transmission of specific instructions on how to break into control systems or (iii) the activation, from abroad, of web sites, platforms and proxies which may be used to provide free access to the Internet.

With regard to this consideration, and especially to the idea that during the recent "Twitter revolutions", many scholars were *critical* of this approach, arguing that in fact most of the *Twitter* and *Facebook* traffic did not originate from states where the revolutions occurred, but from areas in other parts of the world that *bounced* the news of what was occurring, Golnaz Esfandiari's remarks concerning this issue are aimed to highlight five essential aspects:

1. *tweets were circulating* outside *the country in which protest arose*. The scholar testifies that, prior to one of the major Iranian protests of 2009, a journalist in Germany showed her a list of three prominent *Twitter* accounts commenting on the events in Teheran, and asked her if she knew the *identities* of the contributors. Esfandiari told her she did, but the journalist seemed disappointed when the author told her that one of them was in the *United States*, one was in *Turkey*, and the third, who specialized in urging people to *take to the streets*, was based in *Switzerland*. Perhaps, says the author, she shattered the journalist's dreams of a true Iranian *Twitter Revolution* (Esfandiari 2010);
2. *the real importance of Twitter in Iran*. Esfandiari criticizes the fact that the Western media were never tired of claiming that Iranians used *Twitter* to organize and coordinate their protests following President Mahmoud Ahmadinejad's apparent theft of the elections in 2009. Even the American government, writes the author, seemed to want to become involved, with former United States national security adviser Mark Pfeifle claiming that *Twitter* should be awarded the *Nobel Peace Prize* because 'without Twitter the people of Iran would not have felt empowered and confidant to stand up for freedom and democracy'.

The U.S. State Department too reportedly asked *Twitter* to *delay* some scheduled maintenance in order to allow Iranians to communicate as the protests grew more powerful. However, the scholar has a conflicting opinion: it is time to get *Twitter*'s role in the events in Iran right. Quite simply, there was no *Twitter Revolution* inside Iran (Esfandiari 2010);

3. *the importance of traditional means of protest*. The scholar recalls how a number of opposition activists had told her they used text messages, e-mail, and blog posts to publicize protest actions; however, and most importantly, good old-fashioned *word of mouth* was, by far, the most influential medium used to shape post-election opposition activity in Iran. Esfandiari writes that there is still considerable debate on *Facebook* as to how the activists spread information, but *Twitter* was definitely, in her opinion, not a major communications tool for activists on the ground in Iran. Nonetheless, she writes, the *Twitter Revolution* was an irresistible meme during the post-election protests, a story that wrote itself, and various analysts were eager to chime in about the purported role of *Twitter* in the *Green Movement* (Esfandiari 2010);
4. *intense Twitter use by the western media*. Esfandiari notes that western journalists who couldn't reach, or didn't bother reaching, people on the ground in Iran, simply scrolled through the English-language tweets posted with tag #iranelection. Through it all, the author observes, no one seemed to wonder why people trying to coordinate protests in Iran would be writing in languages other than Farsi;
5. *real (and not virtual) sacrifices during the protest*. Esfandiari states clearly that it is not that *Twitter* publicists of the Iranian protests did not play a role in the events of the that year, but simply that the role they did play was not that of the main protagonist, as it is often made out to be. And she remarks, finally, that that has been a terrible *injustice* to the Iranians who did make, and continue to make, real, not remote or virtual, sacrifices in pursuit of justice (Esfandiari 2010).

2.1.3 The Power of Technology in Critical Contexts and the New Public Sphere

The second consideration is that technologies are also *powerful*: since they put into the hands of individuals, who wish to or who need to speak out, truly formidable resources, especially in those realities where the media are, as often happens, state-owned or controlled.

Sartor, *inter alia*, is quite clear about the power of technology in political frameworks and its capacities to create a *new public sphere*, highlighting three fundamental points:

1. *the creation of a new public sphere.* Information and communication technologies (and, in particular, the Internet) have enabled the formation of a new public sphere, where individuals *merge their opinions* and *build social knowledge* in a variety of ways (Sartor 2010: 4);

2. *the rise of new forms of political dialogue*. Not only may individuals engage with one another, as they have always done in face-to-face interaction and debate, but new ways of political communication have emerged, where one can post one's contribution to an unlimited number of hearers, or people can merge their cognitive efforts in a variety of discussions (Sartor 2010: 4); and
3. *the diffusion of real open dialogues*. In a way, observes Sartor, the Internet realizes the dream of Habermas, namely, the idea of polity whose choices result from *open uncoerced dialogues*, under conditions of *equality*, and political dialogues can avail themselves of the evidence accessible through information and communication technologies and of the insights obtainable by processing such data (Sartor 2010: 4).

The third consideration introduced above is more subtle: there is the common belief that operating *behind a screen* might ensure greater security, or allow greater tranquility, than protesting in the street, and can render the subject automatically anonymous and secure.

This is not true: every day digital dissidents are detected, arrested and even killed simply because they have tackled the world of technology without the correct strategies. Hence the diffusion of many guides, some of which I will analyze in detail later in this study, on how to use technologies safely, and on the fundamental role, in the daily activities of dissidents, of secure technological frameworks.

With reference to the *fragility*, and to a number of *missed promises*, of the organization of online activity, a study by Etling, Faris and Palfrey argues that, in some cases, the role of information technology in certain contexts has been *over-emphasized* (Etling et al. 2010); this is made eminently clear by analyzing the *three* typical modes of how protest spreads in the world: (i) *mobs*, (ii) *movements*, and (iii) *civil society organizations*.

These three categories, the authors remark, operate in a context where technologies facilitate the flow of information in authoritarian regimes and assist activists to organize, to collaborate and to connect many small groups, a typical characteristic of protest methods in authoritarian regimes (Etling et al. 2010). The benefits of technology have provided free access to information, which in turn facilitates transparency, allowing debate and criticism of government policy, which then permit new voices to join the debate and to verify facts through citizen journalism, that provide alternative sources of information and reduce government control of information. Perhaps the most important results obtained by activists are the consequential surges in levels of free speech and the opportunities to exercise the right to assembly.

The scholars note, as mentioned above, that the activities of civil society groups are almost always divided into three types: mobs, movements and civil society organizations. Mobs are a collection of individuals who, often thanks to mobile phones, gather to protest, usually with improvised and very rapid events, sometimes lasting up to a few hours. Social movements are more sophisticated in their actions, and plan campaigns with long-term objectives to bring benefits in certain situations or to request intervention, sometimes even legislative. Social movements may take years

to reach the goal, while mobs are lightening fast. Finally, civil society organizations are groups or associations of citizens having as their objects social matters and reforms of all kinds: political, social, economic, professional. Generally, civil society groups have a *permanent structure*.

These three categories are not rigid, and one form may evolve into another during the course of activities. A famous example is that of *MoveOn.org*, an online petition which opposed the impeachment of Clinton, and which has since gone on to become a large progressive political institution. All these initiatives may use the Internet to motivate participants to organize protest actions, to search for new dissidents, to capture the attention of mainstream media; they may exercise significant influence, often due to the protection of freedom of expression.

In authoritarian states the danger associated with these groups is greater, because is very easy to locate and harass these them. The revolt in Burma and the *Green Revolution* in Iran, are two examples of complex events that brought together many of those aspects. In such regions, these groups will be completely efficient only when they are able to avoid the control of their repressive governments, as the mere use of technologies does not decrease the opportunity for the state to use both technology and military force against individuals, groups and their leaders. Indeed, in theory, it is much easier to control the flow of complaints online and offline, and technologies can be used with great ease by regimes having negative intentions. The blogosphere in Egypt is a striking example of a mass opposition that became quite strong, because almost all the various components rallied against the regime *together*, including groups of opponents that are generally considered to be politically distant from each other. Success does not derive so much, therefore, from the use of technological tools, but rather, and as is nearly always the case, from human capacity and ability, and, in these particular contexts, from the ability of new network options to mobilize both large and small groups. There have also been very successful movements combining traditional tactics with the ability to improvise. It is always necessary, however, to focus on *people*. (Etling et al. 2010).

2.2 The Fundamental Role of a Secure (and Peer-Reviewed) Liberation Technology: The *Haystack* Case-History

In all likelihood, the most sensational case of insecurity and danger in the use of technological tools involved *Haystack*, a controversial software program created in 2010 by Austin Heap.[6] The program, which had been conceived to establish secure,

[6] The rise and fall of the *Haystack* project is well described in two articles by Kabay (Kabay 2010a and Kabay 2010b), in a number of considerations by Felten on his original suspicions concerning the security of the software (Felten 2010), and in an article by York (York 2010) on media irresponsibility regarding this issue ("So what of the media's role? Haystack has been billed by the media since last summer as a wonder tool, a silver bullet for the Iranians who need desperately to evade censorship. The truth is that, until this week, no one – neither the media nor the circumvention

unfiltered Internet connections for the people of Iran, oppressed by their government which actively seeks to censure channels used to search for, receive and divulge information and ideas, was suspended while still in its testing phase due to documented security issues. The two main issues of the case, as Morozov so succinctly stated at the time (Morozov 2010b), were that:

1. if someone wants to distribute technology that may endanger lives, he must make sure that the technology is *secure*; and
2. the only good way known to make sure that it's secure is to *let outsiders test* it.

Even the technology on which this software was based was unique; it sought to mask real user traffic by inserting it into a huge quantity of unrelated and apparently innocent data, in order to construct a sort of "haystack", making it virtually impossible for censoring organs to find the "needle" of the single user's activities.

The program's developer was the target of sharp criticism from many corners for not having immediately made *public* the source code on which it was based. Heap, however, repeatedly justified this choice by saying that to have done so would have facilitated its comprehension by Iranian authorities, and, consequently, may therefore have resulted in measures to counteract it.

The *Haystack* project appeared to be extremely attentive, initially, to all security issues involved and to the careful planning of the software's local launch. The project's founder noted that in a number of authoritarian countries, where Internet is rigidly monitored, users often sought to circumvent state filters by using proxy servers to mask their identities while on the web. Heap thought that it might therefore be useful to create secure proxies that Iranians seeking web anonymity could safely use. He began, then, to publish information on his blog on how to operate proxies in a domestic environment, but this only led to a one-upmanship race against the regime, and proved to be ineffective when state technicians began to read his blog as well, and, simply began shutting down proxies as soon they were mentioned.

At a certain point, however, Heap somehow came into possession of a secret document from the Iranian government containing internal operative procedures of the state's filtering software. The diagrams it contained aided Heap in understanding how to proceed, and he went on to devise a sophisticated mathematical formula to hide Internet user's true online destinations inside seemingly innocent bundles of web traffic.

Thus what appeared to external observers (and, it was hoped, to any Iranian monitors) was that the user, who in fact was consulting a particular, possibly unacceptable site, was connected to a completely different and innocuous site containing neutral content, both frequently consulted and permitted in Iran.

---

community – could actually vouch for Haystack one way or the other, because none of them actually saw a copy. No one was capable of speaking to the tool's security or efficacy, and yet, a number of journalists did anyway") (York 2010) and in an essay by Morozov about this so-called *great Internet freedom fraud* (Morozov 2010).

The allure of Heap's software was that, if it functioned as it was meant to, it would constitute a leap ahead of existing technologies such as *Tor*, *Psiphon* and *Freegate* because, in all other cases, monitors can see when those programs are installed and utilized, while *Haystack* was meant to be undetectable to both human and technological monitors, capturing all outgoing connections, encrypting them, masking the data with something else, and providing total protection to its users.

The first difficulties for Heap began, somewhat paradoxically, with the government of the United States; given their restrictive policies regarding exports[7] to Iran, it would have been illegal to distribute the American-made program in that country, despite the fact that it had been specifically designed to promote free speech for the Iranian population. The Department of Defense of the United States, however, in consideration of the program's truly innovative and humanitarian nature, significantly shortened the waiting time, waiving a number of review and control procedures, and granted Heap a license for export to Iran. Shortly after this period, Morozov, among others, correctly voiced significant doubts regarding those events and concerning the announcement by Hillary Clinton, in March, that the government of the United States would grant a license to an unknown company whose software, *Haystack*, would help information *continue to flow freely* into and out of Iran (Morozov 2010b). Because of United States sanctions on Iran, observes Morozov, any American entity that wants to export goods to the country must go through a *rigorous review process*, and the exporter also must be granted a special license by the *Office of Foreign Assets Control* at the United States Treasury Department, with the Departments of State and Commerce often having a part to play as well (Morozov 2010b).

Haystack, Morozov notes, was fast-tracked for speedy approval, and the suspect is that *no government agency* examined *Haystack*'s claims closely, or that no one with knowledge of computer security *scrutinized* the software. The scholar notes that his colleague Jacob Appelbaum found faults in *Haystack*'s code in just 6 h, and given that *Haystack* (i) was granted a valuable license, and (ii) its intended users were vulnerable Iranian dissidents, this appeared to be a case of shocking negligence (Morozov 2010b).

Nonetheless, once Heap had been granted the export license for *Haystack*, in early 2010, he began to introduce the program in Iran. Taking a deliberately slow and cautious approach, Heap first shared it with certain carefully selected and trustworthy Iranian dissidents, inviting them one at a time to test the software's functions. Subsequently, he asked them to share the software with an equally limited number of their friends in turn, in an attempt to carefully limit use of the program to the activists themselves.

[7] See the interesting essay by Bowman on United States export controls for the modern era, referring to e-mails, servers and software (Bowman 2004), and the long, ongoing debate surrounding this issue. The author notes that one of the primary issues driving this debate has been the question of how to balance the largely incompatible goals of promoting commercial exports and ensuring United States national security (Bowman 2004: 325); and the same problem affected software as well because, in some cases, Internet postings of software can be considered *export* (Bowman 2004: 324).

However, in late summer 2010, *Haystack* skidded to a sudden stop. After Heap was named, perhaps somewhat rashly, as the *Guardian*'s *Innovator of the Year*,[8] a number of significant incidents occurred in rapid succession, including the identification of a number of security issues with the program that were clearly confirmed by a member of the *Chaos Computer Club*,[9] and which may very well have endangered the lives of many of the Iranians testing the software.

At the basis of the many criticisms was Heap's adamant refusal to render public the program's source code, which he repeatedly explained as being motivated by fears that to do so would make it easier for Iranian authorities to understand and then block the software. This affirmation is in contrast not only with fundamental security principals, but also with Kerchhoffs' principal,[10] which establishes that a system must remain secure even if "the enemy" were to discover every detail of how it functions, generated both significant disapproval and concern. The situation degenerated even further when a well-known security expert, Jacob Appelbaum of the *Chaos Computer Club*, obtained a copy of the binary code and declared that he had seen the program's source code. In a very short time he was able not only to enter the network but also, and far more importantly, was able to gain access to the "digital fingerprints" of all the computers used by those connected to the *Haystack* network, all potential dissidents.

Morozov, with regard to this important security issue, notes that full disclosure was, at that point, the only way. The scholar obtained a copy of *Haystack* and passed it on to another *Haystack* skeptic, the security professional Jacob Appelbaum, for testing and review, and Appelbaum's conclusions about the software's violation of basic safety principles ultimately led Heap to disable the program (Morozov 2010b). Soon Appelbaum was calling the program "the worst piece of software ever" in a September 2010 tweet ("Haystack is the worst piece of software I have ever had the displeasure of ripping apart. Charlatans exposed. Media inquiries welcome").[11]

The harshest criticism was that the system was, in fact, based on a central point, which, if this were easy to find, would immediately become the principal focus of all monitoring activity: its architecture included a central access point which even hackers with only modest abilities could expose.

The project, much lauded and much acclaimed just a few months earlier, quickly imploded.

---

[8] See http://www.guardian.co.uk/megas/winner-2010-innovator-year-austin-heap. Accessed 5 November 2011. ("Heap is the creator of Haystack, a piece of software which was a key technology used by Iranians to disseminate information outside the country in the protests that followed the disputed election result in June 2009. Heap developed Haystack to open up social networking sites such as Twitter and Facebook, giving voices on the streets a platform, and people in the west a window into a closed-down state").

[9] See http://www.ccc.de/. Accessed 20 Novembre 2011.

[10] In the field of cryptography, the principle stated by Auguste Kerckhoffs in the nineteenth century states that cryptosystem should be secure, even if everything regarding the system, except the key, is public knowledge.

[11] See the text of Appelbaum's tweet at https://twitter.com/#!/ioerror/status/24425326976. Accessed 6 November 2011.

As Felten noted, the ultimate failure of *Haystack* and of the team which designed it was the announcement, near the end of 2010, that they had permanently disabled the project's servers and that *Haystack* would be submitted to an external security review and subsequently re-released in an open source format. The scholar subsequently commented that this decline of the project should come as a surprise to nobody, given that it "exhibited the warning signs of security snake oil":

1. the flamboyant, self-promoting front man (Felten 2010);
2. the extravagant security claims: the super-sophisticated secret formula that cannot be disclosed (Felten 2010);
3. the avoidance of independent evaluation (Felten 2010).

Felten, as a sort of closing statement about this important issue and its public impact, wrote that it is necessary to remember that the majority of tech reporters didn't hype *Haystack*, and that non-expert reporters should have known to be wary about *Haystack*, simply based on healthy journalistic *skepticism* regarding bold claims made without evidence. The scholar is convinced that many of the more savvy reporters shied away from *Haystack* stories for just this reason, but the problem is that the few who did not received undeserved attention. (Felten 2010).

The lesson to be gleaned from such a case is that it is always extremely difficult to provide absolute guarantees for *security*, and that in digital environments even *more caution* is required. Thorough *peer-review processes* and an *open source code* would appear to be the only viable paths to follow.

2.3 Two Key Aspects of Digital Resistance Activities, and Several Case Studies

2.3.1 The Key Aspects of Dissident Activities

In very simple terms, digital dissidence resistance activities may be defined in two ways:

1. the dissident combats, with an intensive use of technology, a situation that he/she finds unacceptable. The rebel uses every means available (Internet, *Facebook*, *Twitter*, SMS, blogs,[12] discussion forums, chat, messaging, cellular phones) to

[12] For example, Hossein Derakhshan, the famous Iranian blogger credited with launching the blogger revolution in Iran. He was sentenced in 2010 to 19 years of prison by Branch 15 of the Revolutionary Courts for anti-State activities (especially propaganda against the regime, cooperation with hostile States, propaganda in favor of anti-revolutionary groups, insulting sanctities and implementation and management of obscene websites). He is now considered by many activist groups, to be a prisoner of conscience condemned only for his opinions and writings. Another well-known Iranian blogger, Omidreza Mirsayafi, died in prison Unfortunately, this type of treatment of bloggers is hardly unique to Iran. The famous Tunisian blogger Hamadi Kaloutcha often pays homage to another Tunisian blogger, Zouhair Yayahoui, who was the first cyber-dissident in Tunisia to die as a result of prison

disseminate multimedia information, even in contexts where this is discouraged or prohibited. Political dissidents, independent groups and citizen journalists operate in this way;
2. the dissident directly opposes the repressive technology locally, in the context in which it is located, or from abroad, in a context with which he/she nonetheless make contact with the repressive situation and technology. In this case, his/her main target may be, for example, a filtering/blocking technology, and the goal may be to access, or to allow others, to free content in other parts of the world. What motivates these dissidents is the desire to be like other people, to overcome the cultural or political closure of the countries in which they, or those they seek to assist, live.

Together, these two macro-categories include nearly all examples of digital dissidence. The contexts may be *political* (opposition to oppressive regimes, actions in support of ethnic groups, or on behalf of minorities that are discriminated against), *religious* (willingness to discuss banned issues), but also *cultural* and *technological* (refusal to accept closed systems code, perhaps state-controlled, or lists of features and approved web sites). The contrast to the closure of on-site technologies usually takes place, however, in order to encourage the flow of communication between activists or to communicate with the outside world and to receive specific information.

Hacktivism, online petitions, site defacement, denial of service and other attacks belong to yet another category. Of course, these types of action may be – and often are – related to protest movements, but they are usually fairly simple to organize and to implement, and, above all, they do not necessarily require or denote true activism, digital dissidence, or dissidence activities.

Digital resistance activity, we will see later, has very close connections to the world of hacking or, better, with that most noble of the hacker traditions: that which gives free reign to curiosity, permitting the unconventional use of unconventional technologies, aiming to augment prosperity but, most of all, freedom.

---

violence. Le Chi Quang, in Vietnam, was sentenced in Hanoi to 4 years of prison for propaganda against the Socialist Republic of Vietnam and communications with foreign states by the Internet. In China the cyber-dissident Huang Qi was sentenced to 5 year of prison, and Liu Di was arrested; in Maldives Ahmad Didi was sentenced to 25 years of prison for insulting the President. In Myanmar the Burmese blogger Nay Phone Latt was given a 20 year prison sentence by the Rangoon Tribunal for offenses to General Than Shwe (15 years for offences under the *Electronics Act*, 2 years for creating public alarm and three and a half years for offences under the *Video Act*). Last, but not least, the Egyptian Karim Amer was recently sentenced to 4 years for criticizing Hosni Mubarak's policies, religious authorities and Islam. As Sambidge reported (Sambidge 2012), in 2012, Kuwait's Court of First Instance sentenced Hamad al-Naqi, 26 years, of a 10-year prison sentence for criticising the kings of Saudi Arabia and Bahrain and allegedly "insulting" the Prophet Mohammed on the social media site Twitter. "The Court convicted al-Naqi on the basis of article 15 of the National Security Law, which sets a minimum 3-year sentence for "intentionally broadcasting news, statements, or false or malicious rumors… that harm the national interests of the state". The Court also convicted al-Naqi for a tweet allegedly insulting the Prophet Mohammed and his wife Aisha under article 111 of the Penal Code, which prohibits mocking religion and carries a maximum 1-year sentence" (Sambidge 2012).

It is hardly a surprise, then, that hacker groups, such as *Anonymous*, speak openly in support of hackers and hacker groups in other states, or if small groups of activists are often very skilled in finding, or are forced to find, new technological means of combatting censorship using hacking techniques.

In many states there is a real challenge going on: on one hand, the state invests in technologies and tools to control, on the other activists study methods to break and force the state to find new methods to censor again. In my opinion, a correct (and complex) definition of digital resistance, *inter alia*, is provided by the scholar Adrienne Russell, outlining *four key aspects*:

1. *the* humus *in which resistance is born and the reaction to an authoritarian status*. Russell notes, first of all, that routine government monitoring of Internet activity in the name of national security, extensive use of firewalls and copyright law to limit access to information, court-ordered seizures of Internet servers and user lists, and arrests and prosecutions of web users and activists around the world have all provided ample evidence that the Internet can be as much a tool of repression as of liberation. Yet, writes the author, online resistance to these and other forms of control continues to evolve rapidly, and technologies that facilitate collective political and cultural practices are shaping Internet use and integrating it more deeply into the lives of Internet users around the world. The means most commonly used to reach these goals are instant messaging, "smart e-mail", collaborative weblogs, wireless wide-area networks, 'wiki' open-editor websites, and social networking software (Russell 2005);
2. *the notion of digital resistance*. Russell, analyzing the approach of the so-called tactical media groups, defines *digital resistance* as a form of protest that mimics the way in which digital technology, in effect, has made information itself a new medium. Mostly, however, resistance has come about through a combination of necessity and opportunity, and many 'digital resistors' have been denied access to information and media products and/or the power to convey and control their message. They resist, the scholar observes, by moving around and through the barriers to and filters of mainstream media and by hacking technological and legal restraints on information, delivering alternative messages to expanded audiences and making new media or using existing media in new ways in the process (Russell 2005);
3. *most common tools used*. The scholar lists four common tools that are quite helpful during protests: (a) social networking sites, (b) file sharing software, (c) blogs, and (d) webcams. In particular, social networking sites facilitate online and offline political rallies and strategy formulation, file-sharing continues to challenge culture industry outlets, blogs function as independent editorial pages, and webcams deliver what embedded network video cannot (Russell 2005);
4. *the "network quality" of the action.* One of the most distinctive features of digital resistance, writes Russel, is its *connected* or *network quality*. Every form of wired opposition, regardless of efficacy or ideology, is now part of the information web, available for copy and adaptation by the vast majority of users everywhere. In the face of fears of a rising authoritarian and homogenous global

culture, these projects underline the independence and plurality that exist in the new media environment (Russell 2005).

This definition highlights a number of key introductory points, most importantly the birth of electronic resistance as a *dynamic* and constantly evolving reaction to oppressive policies and to attempts to control communications and technology, and as an attempt to secure the independence of thought and communications. The term *digital liberties* indicates, among other rights, those manifestations of free speech as applied to the digital world, allowing full and unlimited self-expression. In this last (dynamic) case, reference to the *Digital Liberties Movement* (DLM) is also quite common. Croeser outlines *three* fundamental aspects of the notion of DLM:

1. *DLM as a reaction to control*. The DLM has emerged partly in response to élite attempts to (re)gain control of information and communications technologies, and partly through merges of (and changes within) communities that have existed for decades, including the free/libre and open source software (F/LOSS) movement and the hacker community, that use and develop ICTs. It is primarily concerned with retaining citizens' control over ICTs in the face of corporate and government power (Croeser 2009: 5–6);
2. *the attention to digital liberties.* There are a number of organizations and individuals which form the core of the movement, and, in each case, one could dispute whether "digital liberties" are really the focus of their activism (Croeser 2009: 5–6);
3. *the power of organization and common goals.* These activists are increasingly tying together issues as wide-ranging as online civil liberties, F/LOSS, digital rights management, and intellectual property rights. At first glance, remarks the author, it is difficult to see the connection between these issues, and in many cases their political dimensions are unclear. Establishing that there is a connection, and framing these issues as political, constitutes a large part of the DLM's work. The frame that ties the movement together is the attempt to build an understanding that citizens (rather than corporations or governments) should control ICTs and the online spaces which they have created, tying this control to democratic principles and ideals of personal freedom (Croeser 2009: 5–6).

Once this definition has been clearly established, the concept of digital liberties may then be interpreted in two ways, both of which, in my view, are perfectly correct. The first interpretation emphasizes the term "liberty": *digital liberties* are thus those rights to liberty already established by the regulations of a given state (as provided for, for example, by an existing Constitution), to be evaluated in terms of their applicability to the digital world.

This is a more "classic", legal vision of rights and freedoms (for example, the freedom of speech, the freedom of assembly, the right to confidentiality of correspondence, the freedom of entrepreneurship, the freedom of the press) and it analyzes the ability of these liberties to withstand the changes that occur as we move toward an increasingly digital society.

A second, and equally compelling, approach consists of defining as digital liberties those liberties (of individuals, of citizens, of consumers) which are created and developed in the digital world, using the more traditional liberties and rights as merely a basis on which to construct a new framework of rights and liberties for the digital world.

Examples are bloggers' rights, the right to web anonymity, and the right to participate in file-sharing and peer-to-peer networks.

These new rights, however, cannot truly be seen as constituting a whole new category: they are simply the most modern manifestations of our most classic rights and freedoms, and they have become, over the last few years, the battle cry for many of the most important associations for the protection of civil rights in cyberspace.

It is well-known that, over the last few decades, both those actions actually achieved by, and those only attributed to, hackers have covered every part of the legal and ethical spectrum, and have been ascribed countless shades, nuances and connotations.

I firmly believe, however, that it is not at all difficult to differentiate between purely criminal actions, which have nothing to do with hacking, even when they involve individuals commonly considered hackers, and episodes of true protest, which should clearly be included, with no interpretative difficulty whatsoever, in the category of *digital resistance*. In fact it is only the second of these two categories which can be said to have altruistic aims, often noble aims, which are often most evident in moments of great difficulty and which may sometimes collide with prevailing interests, or menace, directly or indirectly, multi-million state or private investments in technology.

It is for this reason that the actions of those who crack into financial systems, who steal funds, who sabotage organ donor data banks, who are paid by states and corporations to commit espionage, be it public or industrial, or who commit other types of paid misconduct for reasons purely connected to personal gain are, in truth, of far less interest. They are of no use whatsoever for the intellectual and civil growth of a nation or of a people. They are simply, and nothing more than, criminals.

To my mind, far more interesting are the today's modern hackers, who, more so now than in any other historical period, develop anonymity networks, cryptography systems, develop and foster free operative systems, act to circumvent unjust laws, promote the freedom of thought, protect consumers by allowing them to by-pass filters and firewalls, work tirelessly for a culture that is more free overall, seek to assist the disabled in using and keeping up with the world of technology, signal bugs, loopholes and other security shortcomings in public computer systems, the malfunctions in state infrastructure, the technologic inefficacy of political choices, and keep sharp watch on all aspects of our new "information society".

Fascinating, too, are the actions of these individuals, who seek to use technology to hack the current system of "doing politics" and who believe that the only real way to guarantee the proper functioning of the public sector and to fight corruption is true *transparency*.

Similar dedication is found in the particularly praiseworthy souls of those who see as their mission the circumvention of political and technological filters and firewalls created by the states in which they live, who have no access, without resorting to technology, to a culture other than that approved by the reigning political powers, who cannot listen to the voices that modern technology is in the position to allow us all to hear, and who risk their very lives in order to voice their opinions, or for simply seeking to inform.

Equally admirable are those hackers, experts in surveillance and interception, who develop increasingly sophisticated systems to analyze network traffic, and at the same time absolutely believe in personal privacy, and thus develop increasingly non-traceable technologies.

Just as fascinating is the more colorful, dreamier side of the hacker world, featuring conspiracy theories, varying global threats and menaces, cold hostility toward certain technologies and unfettered adoration of others.

Based on these premises, it becomes an easy task to distinguish between actions that seek to reveal information which the citizen clearly has the right to know (including technical vulnerabilities, outcomes of public bid processes and the assignment of funds), and hacking actions which seek to elude or by-pass laws and regulations which are oppressive, or perceived to be unjust.

All these different types of hackers, covering an enormous spectrum, from hot-shot computer super-experts to those who grimly invest in covert action and strategy, taken together make a sort of "digital resistance army", and, on a daily basis, reach countless objectives, some small, some simply huge, all of them continuing the tradition of *rebellion*.

2.3.2 Digital Resistance Case-Studies

2.3.2.1 Cyber-Resistance in Saudi Arabia in the 1990s

In an interesting essay, Fandy describes the first activities and techniques of cyber-resistance in Saudi Arabia, a very complex landscape (Fandy 1999).

The political situation since then has changed significantly, as well as the available technologies in that country in the last 20 years, but the example cited is very interesting not only because it is one of the *first* electronic resistance activities in the world, but also because some basic principles have remained, and raise, highly interesting issues.

Saudi opposition groups in the 1990s, notes the author, were *different* from those in other states both because of the extreme limitations on conventional expressions of dissent within the country and because of the opposition's access to nearly unlimited cash and the global flow of information. They were, Fandy remarks, the first of the opposition groups in the Middle East to make extensive use of new technologies in communicating their message to their followers (Fandy 1999: 126).

The author observes, too, that new technologies and new means of communication had provided opposition groups, as well as the state, with an *intermediate space* and a new means of disseminating information in a "virtual space", beyond their limited conceptual and physical spaces. However, more for the opposition than for the state, the Internet and other media, such as fax machines, cellular phones, satellite dishes, and cassette tapes, provided a new space for dissident activities with minimal risk (Fandy 1999: 127).

In that period there were several important dissident groups. The *Hawali-Auda* Group, first of all, was a group that had emerged during the Gulf War period and that depended mainly on audio and video-technology to communicate its messages, and the *Shi'a Reform Movement* which, as Fandy explains, depended on various media, including cassette tapes, faxes, and limited use of electronic mail.

These were the two main examples of digital resistance activities in the country. Two other groups, the *Committee for the Defense of Legitimate Rights* (CDLR) and the *Movement for Islamic Reformin Arabia* (MIRA), were Sunni groups that made extensive use of the Web and other technology to elaborate a discourse of resistance both outside and inside the Kingdom.

Fandy notes that, in those days, opposition forces and other social organizations frequently circumvented censorship and regulatory institutions in order to acquire or transmit alternative messages; they circumvented the state control of press, radio, and television through the use of satellite dishes, the Internet, and cassette tapes.

Since Saudi Arabia is a very large country, revolutionaries needed to *disseminate* their message throughout this wide space: the author remembers that, with the advent of the Iranian revolution in 1979, the *cassette tape* was introduced as a new means of political communication, and this means became popular in the Sunni regions of Saudi Arabia only in the mid 1980s, intensifying in 1988 and after (Fandy 1999: 131).

Concerning the reaction of censorship institutions, the author notes that the state had limited success in controlling the cassette tape phenomenon; from a legal point of view, the regulation of cassettes, and the shops that were selling them, were covered by the *Press and Publication Code*, which put the matter under the responsibility of the *General Directorate for Publications*. The *Directorate* has sought to counteract the influence of cassette tapes principally by raiding the shops that were selling them, but this has proven ineffective and tape distribution has continued to increase. In response to government raids, activists have turned to underground networks to distribute their tapes, and these networks were based on the existing structure of the clandestine *Muslim Brotherhood* organization, the Hizb al-Tahrir (*Liberation Party*), and the *Salafi* network. These underground networks have been central to the distribution of cassettes, and faxes make the texts of these tapes available to everyone. Fandy cites also the web site of the *Committee Against Corruption in Saudi Arabia* (CACSA), who maintained the best opposition homepage.

In the author's words, the new modes of resistance resulting from the mobility of the site of resistance created a marked difference between a new and "postmodern" resistance and that of the "premodern" era. This is obvious in the case of cassette tapes and cellular phones and of the global flow of information on the Internet.

These new developments have accorded the opposition an opportunity to communicate with similar groups and to learn new strategies from opposition

movements elsewhere and these new spaces allow the opposition greater coordination and communication not available at home. Even if this is not direct communication among the groups, the information is available for anyone to see, copy, or download (Fandy 199: 142).

2.3.2.2 E-Resistance Among Palestinian Women

A second, very suggestive example regarding the status of women in Palestine and their use of technology to overcome hostile political and social situations is described in a very recent study by Shalhoub-Kevorkian (Shalhoub-Kevorkian 2011).

The author explains that cyberspace can serve as a *site of resistance* and a *tool of power* in the hands of the occupied, but that it may also be a *source of danger* when that space is bound to the logic of security, surveillance strategies, and politics.

Examining the role of electronic spaces in Palestinian women's lives, the scholar considers the ways in which such spaces are affected by (and embedded in) a variety of structures, local and global, political and social, and also discusses the relationships between electronic spaces and power dynamics.

The study introduces the concept of *feminist digital resistance in conflict zones*, including in that definition the resistance against external political oppression and against patriarchal oppression in the home (Shalhoub-Kevorkian 2011: 180).

The author, firstly, describes how the introduction of cyberspace and digital technologies can affect the power dynamics in politically contested locations, and may have particular effects on the role of women in those dynamics; and additionally explores how the development of a technological infrastructure that operates on a day-to-day basis and on a global scale can enhance women's opportunities to resist and cope with patriarchal oppression in the domestic sphere, as well as with militarization outside the home. On the other side, technology can also increase crimes against (and abuse of) women (Shalhoub-Kevorkian 2011: 181).

Thus there are two principal concepts in this very informative essay:

1. the Internet as a tool for knowledge dissemination, communication, and outreach may be successfully used to overcome constraints on physical movement and gendered political hardships;
2. the Internet can open new horizons to individuals and groups living in conflict-ridden areas but, at the same time, can also be a tool of distruction and technological oppression, as well as a source of danger and a means of manipulation.

The last portion of the essay, and perhaps the most interesting, explains how the Internet can take the form of a *new site of resistance* and coping for Palestinian women. The Internet, in this particular region, is used by women to obtain permits to cross physical boundaries, to apply for school, to look up medicines, to search for lost relatives, to get in touch with loved ones, and to attempt to find a desired accessory, appliance, or piece of clothing. The Internet is also particularly useful in overcoming restrictions on movement, in helping individuals in occupied areas to maintain contact with family and friends, especially in times of crisis, and in creating ways to communicate with family members, lovers, friends, and classmates, in exile or abroad.

The Internet is also widely regarded as an important means of empowerment: it provides users with a means to compensate for the loss of control over their lives and also functions as a *space* in which to construct a safe haven, so that individuals living under the harsh conditions of a conflict zone can confront and deal with military exclusion policies. Many women perceive the Internet, mobile phones and Skype as methods of sharing loss, coping, and seeking assistance, and in colonized and occupied spaces, the Internet can be a tool for coping with the trauma of losing one's home and may even become a new home in a homeless situation.

The author, using and on-site reports and interviews, makes a final, and extremely interesting point. She encountered a number of young people who use the Internet to write stories about their rights; these stories center on the freedoms of movement, of speech, to participate in family events such as funerals, and the freedom to move about freely and to reach workplaces or educational institutions. At the same time, they also use the web as a space in which they can share their anger, tell their stories, and search for other ways of resisting oppression. This use the Internet, when possible, to ease the effects of oppression and spatial confinement and to share stories, videos, and photographs as a mode of releasing the stress and trauma that they experience in their everyday lives is not only fascinating but also quite inspiring. (Shalhoub-Kevorkian 2011).

2.3.2.3 Digital Resistance as an Art Form : *Critical Art Ensemble* Theories

A third case history is not related so much to social or political issues, but rather to the world of art and culture, and is the interpretation of the concept of digital resistance by the artists' collective known as the *Critical Art Ensemble* (CAE), which has often used this term to describe the approach to their activities.

CAE is a group of five tactical media artists dedicated to exploring the intersection between art,[13] technology, critical theory, and political activism. Their often

[13] See also the study by Lane and Dominguez concerning *Digital Zapatistas* and the activities of Ricardo Dominguez, founder of the *Electronic Disturbance Theater* (EDT) (Lane and Dominguez 2003). The authors describe the facts: "One year later, the Electronic Disturbance Theater had designed the flight plans for a companion digital Zapatista Air Force: the code for its 'ZapatistaTribalPort Scan' (ZTPS) was released for public use on 3 January 2001. With this software, artists and activists could mount their own aerial attack on any web site – the U.S. government, or the Mexican military – sending thousands of messages through the 'barbedwire' of ports open to the cyber network. The messages sent by the digital activists were drawn from a fragmented, bilingual poem about the Zapatista struggle for peace with dignity in Chiapas […] Fragments of the poem are sent with each port scan, so that the targeted system itself will log the text. Because a cyber-protest usually involves thousands – even hundreds of thousands – of participants, the system will begin to repeat and rewrite the poem at incredible speed, composing and recomposing the fragmented world of the Zapatistas in its very own system logs. Comparable to other forms of public protest and civil disobedience in public spaces off-line, this organized event takes place in the publicly accessible spaces of the Internet in order to register a huge collective, politicized presence in digital space" (Lane and Dominguez 2003: 130).

cited "revolution", "dissidence" and "electronic resistance" seek to call attention not so much to revolution *per se* but, as they themselves have put it, to particular historical times

> […] that appear to be more desirable moments to live in than other times – times when issues of autonomy, of voluntary cooperation, and the liberation of desire have greater practical currency (McKenzie and Schneider 2000: 139).

One of the most provocative CAE positions concerns the futility of political activism based solely on the image of sedentary power: that is, power as centered in bunker-institutions, and thus resistance as a matter of *taking to the streets*.

The state, according to their approach, has given people the streets because power has itself gone *nomadic* through electronic networks, and that is why, according to CAE, "resistance must go digital, too" (McKenzie and Schneider 2000).

But, they admit, the problem with electronic civil disobedience, or any type of political action that can have immediate policy shifting effect, is that it can only exist *in absentia*. It is possible, only, to discuss it *abstractly*, and not concretely, because the authorities would promptly arrest everybody involved.

Concerning *Electronic Civil Disobedience* activities, CAE suggests that political cells might contain an activist, theorist, artist, hacker, lawyer, and even a fetishist of bureaucratic efficiency: individuals with diverse technical abilities can be drawn together by common political beliefs and causes (McKenzie and Schneider 2000).

2.3.2.4 Digital Technology and Human Rights: Soldier Photography of Detainee Abuse in Iraq

A 2010 essay by Whitty gives an excellent description of how digital media technologies can provide new opportunities for the *recording* and *publicizing* of human rights violations, focusing on soldier photography during military conflicts and on the visual representation of detainees (Whitty 2010).

The essay deals with the death of Baha Mousa, an Iraqi civilian who died while in detention on a British Army military base in Basra in southern Iraq in 2003. A soldier's video footage of Mr Mousa's treatment in the detention facility has helped to generate a range of cultural, political and legal effects, not least an on-going official Inquiry into the causes of his death.

The author, first of all, outlines three preliminary, but fundamental, aspects:

1. *new technologies of witnessing.* Whitty remarks that the development of new media technologies has had important consequences for human rights law and practice, and the use of mobile camera-phones and compact digital video recorders, allied with almost instantaneous Internet posting, has provided new 'technologies of witnessing' (Whitty 2010: 690);
2. *a concept of human rights visual culture*. More generally, the scholar notes, the concept of 'human rights visual culture ("what do human rights look like?")' is undergoing profound change as digital imagery takes on a central, and even crucial, role. Whether in the context of human rights lobbying and educational campaigns,

publicizing marches and demonstrations or the recording of abuse and victim testimonies, the use of new media technologies is now common practice. Perhaps more significantly, the construction of human rights claims, and the extent of public and media engagement with the issues raised by these claims, can depend on the availability of visual evidence (Whitty 2010: 690);

3. *media across borders*. The scholar's conclusions on this point are quite clear: the ability, in the digital era, to transcend national boundaries and effect a rapid globalization of images is key. As *Time* magazine claimed in relation to the shooting of an Iranian woman, Neda Agha-Soltan, at a Tehran pro-democracy protest in 2009, the mobile phone footage resulted in 'probably the most widely witnessed death in human history'. (Whitty 2010: 690).

Concerning the relationship between new technologies and the human rights field, the author notes that another important questions is raised by this growth of new media technologies in the human rights field, not least their impact on the historic problems of (mis)representation of the victim/violator by the mass media and political elites, and the inevitable contestation over controversial images of violence, suffering or death. In some contexts, writes Whitty, visual evidence, whether or not it is in new digital formats, will not be an influential factor in determining either official reactions or public disgust (Whitty 2010: 690).

The *power* of the electronic materials capturing the Mr Mousa's treatment at the hands of his captors, Whitty remarks, is clear. There were, first of all, two pieces of visual evidence: (i) 46 photographs detailing the 93 separate injuries on the body of the prisoner were presented, and subsequent media coverage centred on one autopsy photograph in particular; the close-up image of Mr Mousa's badly bruised face, and (ii) a 1-min video taken from a British soldier's mobile phone recording showing a hooded and handcuffed Mr Mousa, alongside five other Iraqi detainees in a room, being verbally abused and forced into painful 'stress positions' by Corporal Payne on the day before he died (Whitty 2010: 694). Whitty notes that this material was originally banned from public release by the Judge Advocate at the Payne court-martial on the ground that it would provoke further hostility towards British troops then operating in Iraq but, following its introduction into evidence at the Inquiry in July 2009, it has now been 'replayed countless times on television news bulletins, newspaper web sites and on *YouTube* (Whitty 2010: 694).

The *visual impact* was fundamental in this case and, as Whitty outlines, what is most striking about the Mousa case is the existence of particular visual representations of the *time*, *place* and *context* of Mr Mousa's violent death and, relatedly, the ability to access and re-access this material on the Internet. There are images of Mr Mousa in the hours before and after his death at the hands of British soldiers; there are also images of the detention/interrogation facilities constructed in a war zone, interior environments historically off-limits to public scrutiny. New media technology has, in other words, made visible to a potentially vast global audience of spectators what is usually kept hidden and unknown in wartime (Whitty 2010: 695–696).

New media, the scholar concludes, can subvert even traditional reporting rules because the ability to photograph a war zone generally requires a presence in that

war zone, and only soldiers and military photographers have access to the uncensored sights of the battlefield. Photo-journalism, from its earliest days, has been subject to strict military and political controls; these, in turn, meant that the public's exposure to war images could be regulated and managed. New media technology are challenging these norms (Whitty 2010: 698).

2.4 Open Government, Collaborative Transparency and Civic Hacking as a Form of Digital Resistance

2.4.1 The Idea of Government as a Platform for Transparency

Recent studies on the issue of open government equate transparency and the free circulation of information with the hacker *Do-It-Yourself* (DIY) principle. Thus, the new concept of transparency increasingly views crowdsourcing and the spontaneous and virtuous collaboration of citizens as models for the creation of social and economic value.

In fact, numerous studies maintain that, in order to create an effective open data policy, the first step is to imagine that the government is a platform,[14] simply another provider, furnishing data and services.

As Cass Sunstein stated when presenting a project launched in the United States regarding this issue:

> At the President's direction, this Administration has taken unprecedented measures to promote transparency and open government. We have started to democratize data. Through our government-wide efforts, we are providing people with new access to information and analysis. We are reaching out to them directly for innovative ideas. We are making government a partner with the American people by breaking down the barriers that have long stymied public collaboration and participation. Domains such as records management, which many of you help ensure, play a crucial role in all this by ensuring accountability through proper documentation of government actions (Sunstein 2010).

[14] See the UN *e-Government Survey 2010:* 16: "The idea of 'government 2.0' is generally associated with the use of social media by the public sector. Recently, the notion has assumed greater definition through its association with government as a 'platform' or provider of data and services for others to exploit as they see fit. Advocates for the concept of government as a platform privilege the role that governments should play as providers of web services, allowing third parties to innovate by building upon government data and applications. They believe that if governments provide data in a non-proprietary and predictable format, third parties are more likely to maximize the value of this information, hence providing services that better respond to users' expectations and needs. Consequently, it is claimed that governments should use the Internet to provide free data in formats that are open, structured and machine-readable, while the Web presence of governments is incrementally reduced as third parties start to provide information to the general public". http://unpan1.un.org/intradoc/groups/public/documents/un-dpadm/unpan038845.pdf. Accessed 2 March 2011.

It is evident that such a reflection has connections to the political message behind the free software movement if software liberation, in its two forms of free software and open source, serves to allow developers to study, modify and contribute to source code, in much the same way the government may be considered to be open not when its data and information are simply accessible, but when it too is deemed "common source", and regulated like any other public resource, allowing others to utilize, develop and even to improve it.

The uniting theme with digital dissidence, once again, is the concept of *transparency*, understood as a path toward increased re-utilization, given that the free flow of information consents further development by others in a virtuous and continuous process of improvement.

If, in fact, as evidenced above, governments maintain the majority of all data, the creation of an open platform and the liberation of public data might well consent further exploitation and development of this enormous wellspring of knowledge, as yet unutilized (or at least under-utilized) in order to develop new and previously unimagined public services.

Sunstein identifies *three clear motivations* for supporting the open data and open government approach, and all of these bear directly on record management. These three motivations, according to the scholar, are:

1. *the promotion of accountability*. First, Sunstein notes, open government promotes accountability, and he recalls the words of Supreme Court Justice Louis Brandeis: 'Sunlight is said to be the best of disinfectants'. By putting a public spotlight on the actions of public and private institutions, is possible to motivate significant improvements in performance (Sunstein 2010);
2. *the possibility of discovering really useful information*. Second, Sunstein writes, transparency enables people to find information that they 'can readily find and use'. That is why the President of the United States of America has asked that agencies 'harness new technologies' and 'solicit public feedback to identify information of greatest use to the public'. Through such steps, it is possible to provide people with information that they can use to improve, and even lengthen, their lives (Sunstein 2010);
3. *collective experience and access to dispersed knowledge*. Third, Sunstein notes, knowledge is widely *dispersed* in society, and public officials benefit from having access to that dispersed knowledge' and hence to 'collective expertise and wisdom' (Sunstein 2010).

Sunstein remarks that, through more open, accountable, participatory approaches, the administration is seeking to bridge the gap between the American people and their government and to reshape government according to three core values:

1. *transparency*. Government should provide citizens with information about what their government is doing so that government can be held accountable (Sunstein 2010);
2. *participation*. Government should actively solicit expertise from outside so that it makes policies with the benefit of the best information (Sunstein 2010);

3. *collaboration*. Government officials should work together with one another and with citizens as part of doing their job of solving national problems (Sunstein 2010).

Another important principle, the scholar explains, is the principle of *accountability*: the basic idea is that officials should be held *accountable* for their action and inaction – and that accountability requires transparency because transparency not only improves performance and effectiveness, but it also provides people with access to information they "need and use", thus promoting learning and making data and evidence easy to find and easy to use (Sunstein 2010). In an open government, anecdotes and guesswork can be replaced with *hard evidence* – a point that bears directly on records management. And indeed, that is a central goal of transparency. The third function of transparency, according to Sunstein's analysis, draws on the understanding that no one of us knows what all of us know, and he refers to access to *dispersed information*, to how open government can encourage public participation and allow citizens not just to keep the republic, but to shape it (Sunstein 2010).

2.4.2 *The Metaphor of Government 2.0 and the Idea of Collaborative Transparency*

The suggestive metaphor of *Government 2.0*, without in any way underestimating or downplaying the significant differences between the public and private sectors, allows for a new and powerful concept of *collaborative transparency*, which is rapidly gaining increased visibility throughout the web and which promotes openness as a tool for encouraging the creation of value.

Open data, then, far from being merely the static publication of information, takes on additional value due precisely to its dynamism, representing the first phase of a pathway on which users proceed, independently, to engage in entrepreneurship, to enjoy greater control over community and national political activities, to express opinions and provide feedback and to collaborate in the performance of institutional undertakings delegated to the government and in the betterment of public services.

Added, over the years, to institutional *open government* projects and government data access portals are countless grassroots projects, developed to encourage the transparency and accountability of government activities, augmenting efficiency in the management of the public sector, increasing civic[15] responsibility, improving democracy,[16] combatting corruption and waste in the use of resources, and protecting the users' (that is say, 'citizens') fundamental rights and liberties.

[15] See Jennings and Zeitner analysis of Internet use and civic engagement (Jennings and Zeitner 2003).

[16] See Solop's essay regarding digital democracy during political elections (Solop 2001). The author defines digital democracy as "[…] the integration of Internet technologies into the functions of government and the apparatus of democracy, i.e. making governmental information accessible through web sites; online political mobilization; and, now, Internet voting" (Solop 2001: 289).

These are not, moreover, merely sporadic initiatives, but more and more constitute a true movement which, in homage to the hacker ethic of transparency, understood as an *opening* and as the free flow of information (*information must be free*), is able to gather together, beyond simple data, a multitude of citizens, from all walks of life and all parts of the political spectrum, who see web-based communication tools as a powerful force for change and innovation.

This new model of social production seems not only to undermine traditional and consolidated public service paradigms, on the basis of which services are organized by government and supplied to the citizens (the *collaborator citizen*), but also to use openness and transparency as powerful new *tools* to control the workings of public power and, increasingly, as tools for digital activism and electronic resistance (the *cyberactive citizen*[17]).

Thus, to the extent that transparency can, in the present context, be understood as access, as the openness and free flow of information and as collaborative production, this section will examine how, parallel to institutional initiatives, a silent movement is emerging, especially with reference to the public sector. More than anything else, in fact, this new movement underlines the extraordinary organizing capacities of grassroots and bottom-up initiatives.

Consequently, within the vast and quickly growing movement of digital resistance, I have selected a number of emblematic projects, all of which promote collaborative oversight activities for the purpose of increasing transparency in public policy.

The first category of these projects is comprised of those cases in which the central nucleus of the project is constituted by an online public infrastructure. In these projects, interactivity with citizens is generally stimulated more for integrative purposes, for increased clarity of information, to implement public services in order to personalize them, in terms of time and place, or to improve and develop preliminary projects so that they better respond to the specific need of the citizens.

The second category features those projects arising in situations in which information is not available or requires integration, or in which available information is either not trustworthy or even simply untrue.

These are often projects developed either to overcome public sector limitations, with an aim to utilize collaborative monitoring with institutions as an instrument for improving both the delivery of public services and community well-being in general, or, inversely, projects such as these are often also developed in authoritarian and non-democratic countries with the objectives of digital activism and electronic resistance.

[17] See an interesting Fuglsang's study concerning the use of the Internet for the empowering of active citizenship of *senior citizens* older than 60 in Denmark (Fuglsang 2005). According to the author, "The Internet has been used, with more or less success, to construct elements such as purpose, reciprocal responsibility, manageable framework, feedback, and adjustment of expectations to capacities. It may be presumed that a social learning environment is important to many people who want to remain active citizens in Denmark. For many, IT and the Internet will not become useful tools unless they are explored in a social learning environment. This requires, according to the approach discussed here, a practice context in which active citizenship is empowered. The two projects show how the Internet can be used for that purpose by integration into a practice field". (Fuglsang 2005: 493).

Their distinctive trait is the *originality* of the process of information creation, given that, in order to overcome the lack of available information in a given context, collaborative monitoring becomes the *primary source* of information, and is reconstructed, and re-presented, through the aggregation of thousands of occasional participant contributions.

Miguel, in an articulated paper of 2011, describes the *levels* of government, digital transparency and access of information in South America (Miguel 2011), analyzing the situations in Argentina, Brazil, Bolivia, Chile, Colombia, Ecuador, Paraguay, Peru, Uruguay and Venezuela and the free legal information made accessible to the citizens of these nations by their governments.

The author notes that most of these countries have enacted *transparency laws* to which all government entities are subjected: Chile in 2008, Peru in 2002, Ecuador in 2004, Uruguay in 2008, Colombia in 1985, Argentina in 2003 and Bolivia in 2005. These transparency laws do not only pertain to budget, fiscal, and political accountabilities, but also to free public access to legal information, and the *Organization of American States* (OAS) General Assembly, in 2010, approved by resolution the *Model Inter American Law on Access to Information*.

In Bolivia, access to information, generally speaking, is a civil right, established in the text of Article 21 of the Bolivian Constitution. A presidential decree was issued in 2005 (*Decreto Supremo* 28444) establishing processes and mechanisms for public access to information and transparency in government. In 2006, the Ministry of Justice and Human Rights proposed the *Law of Transparency and Access to Public Information*, but it was not ratified. In 2008, Chile adopted a law on transparency, *Access to Public Information*, wherein Article 7 specifically requires all public organizations to publish certain information, including legal norms, resources, employment, and other information pertaining to its work on its website. The law was implemented in 2009.

Colombia was two decades ahead of its South American neighbors when it enacted Law 57 of 1985, obligating government entities to publish legal acts and official documents. Ecuador implemented its Law of Transparency and Access to Public Information in 2004. The law provides that each governmental entity publish online legal norms that pertain to its work. The law also mandates that the Constitutional Court and the Administrative Court publish their sentences and decisions online In 2002 Peru enacted the *Law of Transparency and Access to Public Information* obligating each governmental body to publish on its web site laws and legal norms that govern its work. In Uruguay in 2008, Law 18381 on *Right of Access to Public Information* was promulgated and requires government entities to make legal information relevant to its work available on its web site in a manner that is easy to find and access.

2.4.3 Citizen Engagement for the Oversight of Political Activity

Projects promoting both transparency as part of the political process and the accountability of government representatives through the simple and efficient mechanism of aggregation of pre-existing public data are increasingly widespread.

This is another very significant aspect of the power of transparency applied to knowledge: in order for published data to be truly transparent, in the sense used in the context of the present work, in some cases further intervention is necessary, consisting of collecting *data sets* retrieved from a number of sources in order to render them accessible, in order that they may be used to provide timely and detailed answers to queries posed by the citizen-users.

Beginning with the literal meaning of the term transparent, that is to say *that which shows itself,* it is understandable how online data becomes visible not only when it is possible to find it and to search through it but also to the extent that it is *easily* found and searched; it should essentially *show itself*.

This aspect becomes very important especially in those cases in which information is beyond the immediate comprehension of citizens, as in the case of public budgets, or when data is easily comprehensible, but not presented in an easily searchable or machine readable form.

To assist with precisely these situations, a number of projects have been developed with the objective of aiding citizens to *read through* the available data and to extrapolate the information lying behind it. A number of these projects have been designed to "crunch" not only open data available in computer readable formats (and thus fairly easy to reutilize for a number of purposes), but also when the target data has not been made available to download in any form and must be "screen scraped" from data available from official sites. In both cases, one key activity of such projects is to contextualize all information received using both mapping and timeline tools, and another key activity common to nearly all these projects is the aggregation of all data received from diverse sources, that is to say, data is gathered and then expressed in summary form.

It is important to point out, moreover, that in this process of the contextualization of data, *users* are not simple data manipulators, but in this context carry out a proactive role that engages them as *prosumers* in a collaboration touching on every single aspect of the project: user contributions may include help with project implementation or unexpected or unanticipated events (even highly technical events!), review of content accuracy (by pointing out any errors and mistakes), enriching the site with comments, multimedia files, links and information acquired "from the field".

In this context, thanks to new technologies, a number of projects have been launched which assist citizen prosumers to discover, explore, re-elaborate, integrate and even to visualize the often abstruse official data put at their disposition by their governments. Much attention has been given to the *personalization of information*, offering citizens, thanks to interactivity and data aggregation tools, targeted search capabilities, statistics, inviting graphics and alerts for real-time notifications of specific matters of particular interest to the individual user.

2.4.3.1 Monitoring Public Spending and Expenditure Mapping

Public spending is constituted by the overall resources used by governments in order to attain their objectives. These are pursued, first and foremost, through budget management consisting of the spending of financial resources acquired through

taxation. It would appear quite clear, then, that the budget is the most powerful instrument available to a government to satisfy the needs and priorities of a country and its population. Historically, however, decisions regarding the assignment of public funds, despite the fact that such decisions directly impact the lives of citizens, have been left exclusively to expert advisors.

Today, thanks to technology, a lively process of change is taking place and placing a powerful *tool for control* in the hands of citizens throughout the world that permits them to prevent cases of corruption and waste and to encourage the well-being and the impartiality of the public sector and the *accountability* of its representatives. Groups of volunteers and civil society associations are launching transparency projects involving the citizens in communities worldwide in the oversight of public spending, in order to influence political choices, to render public budget processes more transparent and more responsible and to allow voters to constantly verify how their governments are utilizing resources gathered through taxation.

The *Open Budgets Initiative* is a global research program conducted every 2 years by the *International Budget Partnership* with the aim of promoting public access to budget information. To measure transparency, and to allow for comparisons among countries, the group created the *Open Budget Index* (OBI), assigning a score, on a scale of 100 points, to each country based on the information it makes available to its citizens. This is based on a detailed survey that gathers data regarding public budget data access in 94 countries.

The 2010 OBI results reveal that 74 out of 94 countries assessed do not respect transparency and accountability norms in the course of their national budget processes. The most virtuous, according to this study, are South Africa, New Zealand, the United Kingdom, France, Norway and the United States. Among the worst, providing little or no budget information to their citizens, are China, Saudi Arabia, Equatorial Guinea and Senegal.

The United Kingdom, with an OBI rating of 87/100, is one of the most open and transparent in the world, although the survey reveals a somewhat worrisome weakness in the UK's budget oversight processes. The timely and detailed publication of data, in this case, made possible a number of initiatives designed to encourage an improved and more accessible presentation of information.

One of the very first of these projects to be created is *Where Does My Money Go?* an *Open Knowledge*[18] initiative created with the aim of making public finance much easier to explore and to understand. Based on the official data provided by the British government and made available on its web portal *Data.gov.uk*, the project is a model of virtuous re-use that demonstrates the advantages of open data in terms of transparency and participation.

Established upon the premise that the answers to many questions posed by citizens may be found only through a process of aggregating and interpreting an abundance of information, and that the effort and time necessary to do so might be a considerable

[18] See http://okfn.org/. Accessed 13 November 2011.

hindrance to those trying to obtain answers, the site provides a concrete description of how British tax monies are spent, and additionally offers a variety of different ways to visualize and compare all available data.

A user-friendly interface even permits tax-payers to identify precisely how (to the pound) their own tax funds are utilized, based on income levels, and to make comparisons between different regions in the country.

The German project *Offener Haushalt* is a similar project created by the *Open Knowledge Foundation Deutschland* in order to make German federal budget data available in a form that is open, accessible and useful. In the absence of open, machine readable datasets available for download, the necessary information is obtained through *screen scraping* this public data from the information published by the Federal Ministry of Finance.

The project *OpenSpending* was created from the fusion of these two projects. *Open Knowledge*'s largest, most ambitious objective is to reproduce the UK model on an international scale and create, its founders explain, an interactive platform containing a world map of public expenditures, on various levels, along the lines of the *OpenStreetMap*, by aggregating public spending data from every country in the world.

In other words, is a project which allows a global public to explore and understand public spending worldwide. The site currently allows vast quantities of spending data to be uploaded, which then may be searched and aggregated; users may additionally use API to create personalized applications and graphic visualization options.

A similar model, but on a national scale, is *Dónde van mis impuestos?* (Where do my taxes go?), created in Spain by David Capo and the *Pro Bono Público Association* in collaboration with the *Open Knowledge Foundation*, promoting budget transparency in Spain. Also Italy's *Open Spending* project has the objective of rendering that country's public data more accessible and understandable. Created by a group of volunteers and unveiled during the "Transparency and Open Data Policy" conference, the project has collected and placed online the open data released by the Italian Ministry of Finance, from 1996 to 2008, in the form of an interactive map.

Understandably, budget monitoring takes on a whole new meaning in developing countries in which the most urgent problem is that of data access. In order to utilize budget data for the purposes of public expenditure monitoring, civil society groups must have access to such information in a timely and systematic fashion. However, many such countries lack both open data policies (and sometimes have very little clarity whatsoever with regard to resource management) and, at the same time, the level of Internet penetration among the neediest levels of the population is still extremely low. In this different social and political context, initiatives often function at an entirely different, grassroots level, seeking to remove obstacles to the publication of data (even in those cases in which certain information is available online, it is often incomplete, unclear and not always reliable), and to inform and educate citizens.

In this sense, the *Ugatuzi Budget Tracking Tool*, an ambitious English-language project from Kenya, is quite interesting. Developed in 2008 by the *Social Development*

Network, it aims to render that country's budget information accessible and comprehensible to everyone.

In Kenya, in addition to the problem of scarce availability of budget information, as evidenced by a 2010 budget transparency index of only 49/100, two other obstacles of no little importance are the low technical skills of public sector workforce and the limited diffusion of Internet among the country's citizens. On the other hand, however, mobile telephone penetration in Kenya has seen important growth in the last few years, and, with a current average of 63.2%, cell phone use is now perfectly aligned with that of other countries. This explains why, even in its initial phases, the project included mobile telephone and especially SMS integration.

With the objective of providing a transparent and proactive approach to the process of public resource management and to the local allocation of resources, the program concentrates in particular on the *Constituencies Development Fund* (CDF) through which members of Parliament assign funds to various projects. The aim is to monitor for cases of corruption and, over the long term, to encourage citizens to proactively manage the public resources of their country so that they can add their own contributions to this area.

Thanks in part to this social mobilization, Kenya is seeing a significant new chapter in budget policy openness: in the year 2011, in fact, for the first time ever, Kenyans were able to provide feedback with regard to the country's budget via social media platforms. Ideas and suggestions, on express invitation of the Ministry, were sent by way of a *Google Document* form incorporated into the Ministry's *Facebook* page.

A Goldstein and Rotich essay in 2008 studied the role of digital networked technology, especially mobile phones and the Internet, in Kenya's 2007 post-election crisis (Goldstein and Rotich 2008) and how digital technology can affect democracy. The scholars note that technologies were a catalyst to both *predatory behavior*, such as ethnic-based mob violence (e.g. text messages urging violence spread across the country, and tribal and politically motivated attacks, or frightening text messages that urged readers to express their frustrations with the election outcome by attacking other ethnic groups) and to civic behavior such as citizen journalism and human rights campaigns, and that while digital tools can help promote transparency and keep perpetrators from facing impunity, they can also increase the ease of promoting hate speech and ethnic divisions (Goldstein and Rotich 2008: 2). The essay describes three important aspects regarding how Kenyans used new technology to coordinate action:

1. SMS campaigns to promote violence;
2. blogs to challenge mainstream media narratives; and
3. online campaigns to promote awareness of human rights violations (Goldstein and Rotich 2008: 3).

On the other side, mass SMS tools are remarkably useful for organizing explicit, systematic, and publicly organized campaign of mob violence. The conclusions of the scholars are clear: in the Kenyan context, whether aspiring to promote an ethnic-based hate crime or a global human rights campaign, the Internet and mobile phones

have lowered the barriers to participation and increased opportunities for many-to-many communication (Goldstein and Rotich 2008: 9).

Another project created to encourage public sector transparency is *Ourbudget*, created in Israel in 2009 by two activists, Noam Hoffstater and Alon Padan, with the aim of allowing Israeli citizens to access and analyze the Tel Aviv municipal budget. In that year, in fact, the Tel Aviv city government, under pressure from the opposition party, published the city's budget online as required by law, but only in *.pdf* format, which rendered very difficult any further processes of elaboration and analysis. *Ourbudget* was developed expressly to allow users to do just that; containing all budget data from 2006 to 2009 on a spreadsheet, it easily permits analysis and further manipulation of the information. Moreover, the Tel Aviv budget data, even when it was published online, was fairly unclear, incomplete and lacking numerous details. In order to change the system, educate citizens and to convince the city's administration to publish more complete budget information in machine readable formats, supporters of the project created an online petition that eventually induced the city hall to publish all Tel Aviv budget data online in *Excel* format files.

2.4.3.2 Monitoring Political and Legislative Activities: The New Active Cyber-electorate

Collaborative monitoring has proved to be a powerful weapon in the defense of transparency and democracy for political and legislative activities as well. Thanks to new technologies, electors now have at their disposition a vast array of quick, user-friendly tools that allow citizens to oversee democratic processes and the political efforts of their representatives.

The first project in this sense was *GovTrack.us*, created for fun in 2004 by Joshua Tauberer, a young programmer and linguistics student, and today managed by the *Civic Impulse LLC Association*.

Nearing its second version, the site boasts over a million visitors each month and makes available a variety of information automatically gathered from diverse official government sites, including *Thomas*, the site of the *Library of Congress* of the United States, active since 1995.

Based on the premise that, for the political layman, it can often be difficult and even discouraging to understand what is occurring in Congress and to follow the path legislation on its way to becoming law, *GovTrack.us* provides a list of bills currently before Congress, lists and dates of votes and other official information on the activities of every single representative, rendering them both easier to understand and easier to compare. It is possible to see statistics for every legislator, including voting tendencies, percentages and absences. The information may be personalized in numerous ways, with the possibility to sign up for alerts, via e-mail, RSS feed or *Twitter*, for updates on individual bills and resolutions and members of Congress.

Data sets obtained through this site are reutilized by diverse open access websites with similar aims, such as *OpenCongress*, *OpenSecrets* and *Facebook* pages such as *Laws I Like*.

In particular, *OpenCongress* is an open source project created in 2007 by the *Sunlight Foundation* and by the *Participatory Politics Foundation,* two of the most active organizations in the field of dynamic Internet-based collaboration for political participation. This project, too, combines official data and social wisdom for the purposes of promoting civic participation and facilitating public oversight and understanding of the activities of the Congress of the United States. Thus, users may track connections between campaign fund contributors, the content of specific bills and resolutions and the votes of the members of Congress.

OpenCongress is based on the aggregation and combination of official government data with other sources such as blogs, social networks, public comments and other citizen participation platforms with the aim of offering the most complete, comprehensible and reliable source of Congressional activities. Information is aggregated, using automated processes from sources across the web, such as *GovTrack.us*, and from the blogosphere, such as *Technorati*, *GoogleNews* and *Google BlogSearch*. User participation is actively promoted and proposed through a user friendly interface featuring nearly all the collaborative tools currently available for peer-to-peer communication, including a commentable blog, discussion boards, an editable *wiki*, and the possibility to share all content on social networks. The site offers particularly high levels of user personalization: *MyOpenCongress* allows users to open individual accounts and to create personal profiles featuring real-time updates on specific issues of interest, to contact representatives, comment on bills and proposals, and follow the entire process through diverse alert and subscriptions features. The aggregation of diverse sources of information and collaborative monitoring by users assures that the site is continuously updated.

TheyWorkForYou, one of the first of such projects created in Great Britain thanks to the efforts of a group of volunteers, is now managed by the British association *Mysociety*. In this case as well the heart of the system is constituted by open source software which automatically aggregates official data rendering it legible, comprehensible and searchable by its users, who are also offered location-based oversight options (inserting a particular postal code calls up the parliamentary representatives). The site offers extremely high levels of personalization, with updates on issues of interest or specific members of Parliament via e-mail or RSS feeds and is quite interactive as well, with the possibility of leaving comments, feedback and suggestions. The site allows users to view a complete updated dossier of each member of Parliament, indicating their principal activities, voting record, speeches and appearances, and expenses claimed. The "Write to Them" section allows users direct interaction with their representatives.

An Italian version of this project is called *Openpolis*, created by the non-profit organization of the same name and managed by a group of volunteers. It allows collective oversight of the activities of all political representatives, from the European Parliament to any Italian municipality. Based on official data acquired automatically from the web site of the Ministry of the Interior, users may view a page for each of the nearly 150,000 representatives currently in office featuring a profile of the politician (personal information, offices held, political party affiliations) and a collection of the politician's principal public speeches and comments. Given

that it is an enormous data base, subject to frequent updates, the collaborative oversight is particularly important in this peculiar case in order to ensure, in a process of continuing improvement, a constant revision and integration of available public data.

Applying a consolidated model of distributed editing, site users take on the double function of information providers (a section dedicated to this invites users to add contributions and links) and editors, guaranteeing the reliability and accuracy of the information and updating sources (through the signaling of errors and a constant process of integration).

The same organization has also created *Openparlamento*, allowing oversight of the activities of all members of both houses of the Italian Parliament, including attendance, voting history, speeches and legislation presented, and additionally permitting user to monitor the process of legislation as it progresses.

Another similar project has been created in India as well. *Govcheck*, still in its beta version, aggregates information from screen scrapings of diverse official government sites (such as *Lok Sabha, Rajya Sabha* and the *Indian Electoral Commission*), with the aim of rendering all such information both searchable and consultable so as to clearly depict the efforts and performance of every single representative of the Indian Parliament.

Although the project is similar, in many aspects, to models having the same intentions developed in Western countries, this particular project must necessarily be contextualized to a society that is not organized around technology. While the open data movement is slowly picking up speed in India, and 2005 saw the issue of the *Right to Information* (RTI) *Act* guaranteeing the right to information, currently in India there are no easily accessible and open public data banks that are re-utilizable (for example, featuring open and machine readable formats), comprehensible (the material published on Indian official sites, to the contrary, is often only available in *.pdf*, or over a number of different sites or published only in aggregate form) and reliable (the absence of clear data collection methodologies leads to significant doubts as to the reliability and accuracy of its sources).

As is evidenced in a recent report on open government data in India, issued by the *Center for Internet and Society* in Bangalore, there are numerous obstacles to the openness of government data, from data gathering phases, not only because the automation of these processes has not yet reached all levels of government but also due to the fact that the data collection processes are still so unclear, to the lack of education regarding the benefits of open data in the public sector (thus when budget information is made available, it is often in the form of scanned *.pdf* files or in aggregate form) and inadequate computer literacy level, especially among the poorest members of the population.[19] To the preceding elements must be added another, the low Internet penetration rates in India: as detailed in a *Boston Consulting Group*

[19] See the *Report on Open Government Data in India*, by *Centre for internet and society*. http://www.cis-india.org/openness/publications/ogd-report. Accessed 7 November 2011.

report, only 7% of India's population has access to Internet, and, although 60% possess a cellular phone, only two million users (less that 0.1% of India's population) use the Internet.[20]

In this context, projects like those outlined above can become, in the mid-term, an important factor for increased social innovation, given that they are limited to simply making official data more comprehensible and searchable, but they represent a tool for exerting pressure on the government and an incentive for increased computer literacy of the country's citizens and greater awareness on the part of the public.

2.4.4 Collaborative Mapping and Digital Resistance

2.4.4.1 Digital Activism in Public Sector

The ever increasing diffusion of mobile communication technology has favored the creation of a number of grassroots volunteer projects utilizing free software and very effectively combining web and mobile telephone technologies to gather and share information, provided directly by user-participants via crowdsourcing tools, for the purposes of activism and electronic resistance.

Over the last 3 years, a movement has arisen that views social media as an effective tool to encourage transparency and combat corruption, to document incidents of violence, ethnic cleansing and terrorist attacks and threats, to manage humanitarian emergencies and to facilitate rescue efforts in areas affected by natural disasters. Every episode, no longer filtered through media intermediation, is portrayed to the entire world in real time, raw, uncensored, through photos and videos uploaded to the web by *netizens*, while a web of tweets, like so many small pieces of a mosaic, viewed together furnish so many new and previously unavailable views, and truths, of even remote corners of the world, that are constantly updated and adjourned.

Citizen journalism is extremely significant especially in countries in which lack of information renders participation in political processes difficult, or, and perhaps even more so, under authoritarian, non-democratic regimes where the right to information simply does not exist or is not protected. It is just this absence or lack of institutional sources of information that has rendered a number of projects created by non-profit organizations or small groups of activists particularly useful and significant; encouraging and then aggregating contributions from multitudes of occasional witnesses, they promote transparency by denouncing public sector abuse and wrongdoings, often visually, and in real time.

An analysis of some emblematic case studies, as pointed out previously, is often quite interesting, both in terms of examining services offered to users and with regard to the process of constructing information.

[20] *ivi*, p. 13.

Projects in the first category, while still relative to the public sector, are created for the purposes of digital activism, generally against (corrupt and repressive) governments, or in any case in order to expose violence and crime of all types. The volunteers involved, in fact, are in most of these cases prompted by the desire or need to create an actual digital resistance platform, or, in other words, to organize a strategy for digital rebellion. Thus transparency and collaboration are utilized to oppose repressive governments, to defend fundamental rights and liberties and to promote collaborative transparency against repression and censorship.

The most innovative feature of the projects belonging to the second category, on the other hand, is the sources of information used: while these projects often deal with information that, for the most part, is already in the hands of government authorities, these activists prefer to reconstruct it *ex novo,* through the aggregation of reports sent by citizen-participants.

2.4.4.2 Elections Oversight as a Form of Digital Resistance

Equally interesting, with a view to increasing transparency, are the numerous projects developed to monitor the events accompanying political elections, especially in countries in which traditional sources of information are not in the position to adequately portray what occurs or deliberately provide information that is not complete, or simply not true.

Given that one of the problems confronting developing countries, is, as has been seen in the previous pages of this book, the lack of information, the mechanism of collaborative transparency is crucial for the collection of reliable reports and testimonies from local citizen witnesses, often in the form of visual evidence to shed light on corruption, electoral fraud, violations of human rights, and episodes of ethnic cleansing.

A feature common to the majority of these projects is the additional graphic representation of incoming reports, placing them on interactive maps or timelines that thus permit visualization of the geographic areas involved and chronological placement in time of events as they unfold.

Representative, in this sense, is the *Sudan Vote Monitor* project,[21] created in 2009 by Fareed Zain and the *Sudan Institute for Research and Policy* in order to aid citizens in monitoring the electoral process during the 2010 elections and subsequent referendum of January 2011.

The objective of the project, set out in both English and in Arabic, was to utilize information and communication technology in order to encourage independent monitoring and reporting on the referendum, recounting the process as it occurred in the various venues, shedding light on any episodes of violence, fraud or irregularity, exclusion of votes and any other difficulty, such as unannounced sudden closures to

[21] See a preliminary report at http://www.mobileactive.org/files/file_uploads/SudanVoteMonitorReport.pdf. Accessed 5 November 2011.

logistic difficulties in handling and protecting ballots. The project permitted anyone to make a report via e-mail, SMS or even to file anonymous reports directly on the projects web site, providing a short description of the event, the date and time, the source of the information and indicating the location directly on an interactive map and with the option of uploading photos and videos documenting the event. Thanks to the work of a dedicated group of volunteers, all reports were mapped in real time and posted to the site. The widespread availability of mobile technology allowed nearly constant citizen oversight of every polling station throughout the country.

This project, like many others of its type, uses *Ushahidi*, which in only 3 years since its creation has become one of the most widely used collaborative mapping programs in the world.[22] The system on which it is based is surprising in its ingenious and linear simplicity, and functions in essentially three phases: the collection of information via mobile telephones or directly onto the web, the aggregation of the same onto a single platform and, finally, its posting, in aggregate form, on maps and timelines. This leads to the creation of databanks featuring thousand of direct reports, thus permitting events to be followed, monitored and better understood as they unfold, in real time.

The extraordinary efficiency of the project and its flexibility and adaptability have assured its use around the world, in a multitude of different contexts, countries and cultures, from xenophobic violence against ethnic minorities in South Africa, to election oversight in India, war reporting in the Democratic Republic of Congo, earthquakes, floods, and other natural disasters and emergencies.

Moreover, the *Ushahidi* project is not simply a collaborative platform, but exemplifies, in its very simplicity, the true essence of the evolution of the *Web 2.0*, and demonstrates, even from a purely geographic point of view, how a simple technology, developed in one of the most disadvantaged regions of the world and promoted at the grassroots level, does in fact, as hackers have always known, have the potential to benefit humanity.

The *Ushahidi* platform was extremely useful during the 2011 presidential election in Nigeria, and was used for the *ReclaimNaija* project[23] which allowed Nigerian citizens to monitor the election process in their country.

The platform, similar to other cases, utilized user reports sent by SMS, mobile phone, *Twitter* or an online form available on the project's website. The *ReclaimNaija*

[22] See, *inter alia*, the article by Giridharadas (Giridharadas 2010) about this "idea of an Internet mapping tool to allow people anonymously to report violence and other misdeeds" and how "*Ushahidi* suggests a new paradigm in humanitarian work. The old paradigm was one-to-many: foreign journalists and aid workers jet in, report on a calamity and dispense aid with whatever data they have. The new paradigm is many-to-many-to-many: victims supply on-the-ground data; a self-organizing mob of global volunteers translates text messages and helps to orchestrate relief; journalists and aid workers use the data to target the response". Additionally, the economic point of view is interesting: "Because Ushahidi originated in crisis, no one tried to patent and monopolize it. Because Kenya is poor, with computers out of reach for many, Ushahidi made its system work on cellphones. Because Ushahidi had no venture-capital backing, it used open-source software and was thus free to let others remix its tool for new projects" (Giridharadas 2010).

[23] See http://reclaimnaija.net/. Accessed 5 November 2011.

project, furthermore, also represented an important source of online information for Nigerians who desired to learn more about their country's constitution, electoral laws, candidates, the country's voting precincts and polling places and, finally, about the results of the elections, which could be viewed interactively based on a number of diverse criteria.

The model has been exported to a number of other countries as well. One example is a Brazilian project, currently still in its beta version, *Eleitor 2010*, developed by a group of volunteers coordinated by Paula Góes and Casaes Diego with the aim of encouraging collaborative oversight for the 2010 elections. In this case, as well, the fundamental elements were the visual testimony provided by voters and their desire to render the process more transparent, by sending reports, photos and videos. The project, implemented entirely in Portuguese, the native language of Brazil, for the first time in that country's history permitted Brazilians to monitor their elections using crowdsourcing techniques. Here, too, users participated by sending reports of misdoings (abuse, polling place irregularities, violence, vote buying, threats) via email, *Twitter* or from a page on the project's web site (for economic reasons the Brazilian project did not include SMS reports). Users could also indicate a specific place of interest on an interactive map and receive SMS, e-mail or RSS feed updates anytime a report was sent from any venue within a range of 20 km.[24]

Ahead of the Bulgarian presidential elections of October 2011, the *Institute for Public Environment Development* of Sofia has created a new project, *For Fair Election*. Available in Bulgarian, English and French, the site represents an advanced model of crowdsourcing, based on the *Ushahidi* platform. Uniting on a single platform all the available tools for social networking, its aim is to shed light on election irregularities, such as electoral fraud, vote buying and voter intimidation. Close attention was paid to both the possibility of exploiting viral sharing on social networks (not only the most common such as *Facebook* and *Twitter*, but also the newer *Google* + and the Bulgarian network *Svejio.net*) and making interaction tools directly available to users on the project's website. Thus the project has prepared a number of downloadable apps, for smartphones (*iPhone*, *Android* and *Windows* and mobile phones with supporting *Java*) that users may utilize to upload reports.

One of the advantages of using a model that is by so well consolidated is that the project developers could give close attention to the few weak points of the process. One of these is undoubtedly the need to provide for the cross-verification of reports and information sources. Every report, therefore, is listed as "confirmed" only when supported by at least two sources or by multimedia documentation. Special verification is reserved for the mapping of incoming reports, which offers a much higher level of accuracy both with regard to the tools available during the reporting process, enabling users to indicate venues with considerable precision (a precise geographical point, an area, or even a single street) and in the presentation of the reports, which reflect the same precision used in their creation.

[24] On the other side, Sampaio reported (Sampaio 2012) a case in which some protesters' accounts on Facebook were blocked in Brazil during the *Marcha das Vadias*.

Another sector in which transparency and collaborative oversight have been very effectively used together to promote democracy and to reduce corruption is that of campaign financing. *Képmutás*, which in Hungarian signifies "hypocrisy", is a project created in 2008 to promote greater transparency in electoral campaign financing. An Argentinian project, *Dineroypolitica*, created during the 2009 elections by the *Poder Ciudadano Foundation*, consists of an interactive data bank and a wiki that aggregate databases in 23 different provinces in real-time and tracks the 713 political parties recognized in Argentina in order to shed light on electoral campaign financing.[25]

The project illustrates the relationships between money and politics, providing data that is easy to understand and to compare, with the aim of augmenting transparency and combatting corruption.

2.4.4.3 Monitoring the Violation of Human Rights

A recent study by Mouza and de Soysa examined the link between several types of communication tools and the levels of respect for human rights in 137 countries around the world (Munöz and de Soysa 2011). From this analysis, it emerged quite clearly that Internet access and the spread of mobile phones offer both more significant opportunities and greater guarantees of democracy as compared to older media, such as television.

In fact, as De Soysa explains, television is actually *negative* for human rights, because it is the preferred means for governments to feed propaganda to the population; Internet and mobile phones seem to have the opposite effect, and in this new scenario, social media such as *Facebook* and *Twitter* play the largest roles, because they give people free access to channels of communication without allowing the government to monitor what they are reading on the Internet.

The conclusions of the authors in this study are clear, and may be divided into several points:

1. *positive effect of the Internet*. There is a certain amount of clear evidence, the authors note, suggesting that the effect of Internet access is *positive* for human rights, net of several important control variables, such as income and regime type (Munöz and de Soysa 2011: 1327–1328);
2. *old technologies take more control*. The older information and communication technology, such as access to televisions and mainline telephones, is negatively related to better rights, suggesting that these older technologies likely give autocrats greater control over citizens. This means that, after controlling for a host of important factors, the old technology lowers rights while the new technology increases respect for human rights. The authors also suggest that, perhaps,

[25] See http://www.dineroypolitica.org. Accessed 13 June 2011.

George Orwell had it right when he saw state propaganda with the effective use of images and the radio enabling mind control, but he possibly could not have foreseen connectivity of individuals among each other as the Internet has allowed in modern times (Munöz and de Soysa 2011: 1327–1328).

3. since the incidence of repression does not allow the scholars to identify whether or not it occurs due to higher dissidence (mobilization) or whether the technology 'pacifies' people (demobilizes populations), they examined conditional effects of new technology with autocracies, which are known to lower rights, and they found that the effects of autocracies on human rights are leveraged downwards on political repression with higher Internet access, suggesting that the new ICTs have effects that are not negligible (Munöz and de Soysa 2011: 1327–1328);
4. their results taken together find support for arguments that suggest that new technologies perform better than old ones, because access to tools, such as the Internet, empowers civil society over states, raising the cost for states to repress rather than reform (Munöz and de Soysa 2011: 1327–1328);
5. the new technologies may very well allow fast and transparent access to areas of human rights abuses and elicit a greater, faster response to such abuse from a global human rights community. Naturally, the authors remarks, the spotlight of global opinion can have severe costs on regimes because of international norms and institutions. This is a positive finding for policy because donors and other agencies can encourage greater access to new technologies, particularly access to the Internet and mobile phones for reducing human rights violations. The spillover is also bound to be positive for creating the virtuous cycle of growth of civil liberties, good governance and economic development (Munöz and de Soysa 2011: 1327–1328).

Since 2009, the ever increasing practice of citizen journalism, fostered by the growth of mobile technologies, has encouraged experiments aiming to exploit the power of collaborative monitoring and oversight process in order to document violations of human rights.

In March 2011, *Amnesty International* created a pilot program, called *Report on Human Rights Violations in Saudi Arabia*,[26] using *Crowdmap*, developed by *Ushahidi* to track human rights violations in Saudi Arabia.

The objective is to create a collaborative map of events, consenting users to report (via SMS, *Twitter*, or directly via the project's website) and locate numerous types of human rights violations, including torture, discrimination and violence against women, the killing of demonstrators and activists, kidnappings and executions.

The different kinds of abuse are divided into categories, each of which is assigned a color, and episodes of which may be easily viewed on a map of the country and on a timeline featuring every incident reported.

[26] See https://amnestysaudiarabia.crowdmap.com/main. Accessed 19 November 2011.

The words of Salil Shetty, the Secretary General of Amnesty International, in the 2011 Report *Activists use new tools to challenge repression* are significant.[27] In fact, Shetty declared that 2010 was the year in which activists and journalists utilized new technologies to *bring truth to the world of power*, making it increasingly difficult for governments to ignore the growing calls for change.

Activists have harnessed the power of information, utilizing new communication technologies, now widely available on mobile phones everywhere, to promote citizen involvement, encourage revolts and to fight for freedom and to demand justice. However, Shetty goes on to point out that technology only offers tools, and that the use of the Internet and other communications technologies are not a magic bullet solution. Technology neither respects nor weakens human rights. It is and will continue to be a tool used both by those who desire to challenge injustice in the world and by those who seek to control access to information and to eliminate dissenting voices.

The Report suggests that we must be mindful that, in a world of asymmetric power, the ability of governments and other institutional actors to abuse and exploit technology will always be superior to the grassroots activists, the beleaguered human rights advocate, the intrepid whistleblower and the individual whose sense of justice demands that it must be possible to access information, or to describe and document a given injustice through the use of these technologies.

This prototype was preceded by a number of grassroots projects aiming to use collaborative transparency as a means of *disincentivizing* human rights violations.

An example of this approach is *Sithi*, which in Khmer, the official language of Cambodia, means *rights*, launched in February 2009 by the *Cambodian Center for Human Rights* (CCDU).[28]

The ambitious objective of this portal is to monitor incidents of human rights violation in that country, to encourage the use of new technologies to increase transparency, and to create a citizens' network based on trust and collaboration.

In a country in which not only Internet penetration is still extremely low (approximately 0.5% in 2010), due to, among other factors, the high costs involved, but freedom of expression and freedom of the press are also tightly controlled by the government,[29] which engages in more or less explicit forms of Internet censorship, using site blocking and content filtering, often with the cooperation of mobile telephone operators, the widespread availability of new communication technologies and increased access to information are powerful tools for the protection of human rights and promotion of democracy.

This is evidenced by the growing presence, even in Cambodia, of numerous *cloggers* (the term for blogger in Cambodian) and web sites for information sharing on important political and social issues.

---

[27] See http://www.amnesty.org.au/report/comments/25630/?. Accessed 13 November 2011.

[28] See http://sithi.org/. Accessed 19 November 2011.

[29] See Virak's essay regarding Internet censorship and the ongoing crackdown on the freedom of expression in Cambodia (Virak 2011).

The aims, set out in both English and Khmer, of the project, which today has the support of numerous partners, are twofold: the project seeks both to encourage the efficiency of civil society human rights organizations and to stimulate resource sharing and cooperation, while, at the same time, also aims to track human rights violations, exploiting the power of transparency to mobilize the country's population and to promote the collaboration of the government.

Over the course of the last year the site's activities have grown tremendously, and its efforts have contributed to the distribution of a great deal of information and publications on human rights violations, which have subsequently been re-utilized by a number of non-governmental organizations and institutions for their own reports on the country. Accompanying the growth of the site's activities has been the number of its visitors, reaching 241,156 in August 2011 alone.

With no official government data available, the information gathering phase, differently from similar projects in other countries, occurs principally due to the efforts of diverse NGOs operating in the area.

Thus incoming data, in the form of area monitoring and first-hand reports filed with the project, is first aggregated and then published on the site, where it can be both visualized on a map and searched based on a number of different criteria.

2.4.4.4 Digital Transparency as a Weapon to Combat Public Sector Corruption

The power of collaborative transparency, as we have seen, is now being used for myriad of projects around the world; among these are a number of fascinating initiatives developed with the objective of shedding light on cases of public sector *corruption* and graft.

In India, for example, a web site, which after little more than a year from its creation has developed a wide following not only within India but internationally as well, has reported incidents of corruption and recounted the stories not only of those who have been compelled to pay bribes but also of those who have refused. The project is called *I Paid a Bribe*,[30] and public response has been overwhelming, with 12,000 reports recorded in the year since its creation. The English-language project was launched on 15 August, 2010 by *Janaagraha*, a non-profit organization headquartered in Bangalore, and seeks to harness the collaborative energy of the citizens of India in order to combat corruption. At its site, users may file three different kinds of anonymous reports: "I paid a bribe", "I didn't pay a bribe" and "I didn't have to pay a bribe".

The project has two principal objectives: on the one hand, the reports filed by India's citizens permit real time mapping of corruption in India, which in and of itself is invaluable, but, at the same time, the project also hopes to raise awareness of a widespread phenomenon that often creates and fosters social injustice, and to

[30] See http://ipaidabribe.com/. Accessed 19 November 2011.

inspire citizens to stand up to the abuse of public officials and to recount their stories of public sector corruption. In order to encourage participation, it was of course first necessary to assist individuals in overcoming cultural resistance and, in some cases, fear. Thus the site's homepage invitation appeals to heart, mind, and civic sense: "Bribed? Didn't bribe? Victimised? Angry? Report your bribe. Tell us your story. Using stories we'll advocate with government for an improved system".

Reports may be sent directly from the site, www.ipadabribe.com, where the user indicates the city, the public sector department, the type of corruption to register, the type of transaction involved, the amount paid and the date, in addition to a brief description of the incident. In order to avoid any chance of retaliation, users making reports are never asked for their own names or those of the public officials involved. In order to create a complete view of the phenomenon in India, site users may select from three different reports: one for victims of bribes, one for those who were asked to pay but did not, and, finally, another for those who have "come across an honest public official" and were not asked to pay anything, and would like to offer positive feedback of good government practices. All reports are aggregated and analyzed, revealing a comprehensive and highly informative snapshot of the status quo: the most corrupt public service departments, the methods used by public officials when asking for bribes, the cities with the highest levels of corruption, etc. With the information provided by site users, the association then intercedes on behalf of India's citizens, contacting the public departments involved in corruption and urging them to intervene.

The site features high levels of user interaction, with the possibility to leave comments, to participate in discussion boards or to follow project on a number of social networks, including *Facebook*, *Twitter* and *Orkut*. An addition section, entitled "Ask Raghu" allows site users to have specific questions answered by T.R. Raghunandan, the project coordinator and former public official. This section currently contains the answers to over 1,000 user queries, ranging from clarification on the workings of the site and suggestions for improvement to requests for advice on what administrative procedure to pursue and even requests to create similar projects in other countries. All are open to user comment. The problem of source verification is resolved by the very nature of the platform: the reports are so anonymous as to discourage any untrue statements.

Recently, the fight against corruption in India has become a veritable social movement, accompanying the progress through India's Parliament of a wide-reaching anticorruption proposal,[31] the 2011 *Lokpal* Bill, whose debate and subsequent approval was preceded by a public consultation via an especially designed dedicated web site which collected input from the entire country. In this context, as well, the Internet proved to be a powerful tool for mobilizing and recruiting activists.

Similar to these projects is a Russian site,[32] *RosPil*, a true venue for investigative citizen journalism, which aims to expose cases of public employees utilizing state

[31] See the text at http://www.thehindu.com/multimedia/archive/00741/Official_Text_of_th_741817a.pdf. Accessed 5 November 2011.

[32] See http://rospil.info/. Accessed 7 November 2011.

funds for private purposes. The project, set out entirely in Russian, was developed by the 34 years old attorney and blogger Alexey Navalvy, nominated *Person of the Year* by the Russian business newspaper *Vedomosti*, and dubbed the Julian Assange of Russia. Seeking to shed light on Russia's public sector tender processes through the efforts of thousands of "normal" citizens, the project invites users to review public tender documents. Any visitor to the site can submit a report, and project participants can also download and use *iPhone*/*iPad* and *Android* applications to file reports, compiling an online form containing a link to the tender (still open and with a deadline no earlier than 3–4 weeks away) and the specific suspicions regarding it.

Hellström outlines also an interesting side-project of political mobilisation conducted by the *Anti Corruption Coalition* in Uganda (ACCU) (Hellström 2011). The name was *Save Mabira Forest* campaign: the ACCU, together with other civil society organizations, mobilized the citizenry to oppose government plans to give away one third (roughly 70 km^2) of the *Mabira Forest* to the *Sugar Corporation of Uganda Limited* (SCOUL), owned by the *Mehta Group* (which to 51% is owned by the Government), for sugarcane plantations. Hellström remarks that the most successful part of the campaign was to urge people, through SMS, to *boycott* sugar produced by the company and the government consequently suspended the idea of giving away the forest (Hellström 2011: 173).

In Cambodia, on 8 February 2009, access to the web site of the UK-based corruption watchdog *Global Witness* was blocked for some local Internet users following the organization's release of a report – *Country for Sale* – on the nascent oil and mining industries (Virak 2011: 4).

A recent study by De Beco analyzed the process of *monitoring corruption activity*, and its relationships with human rights issues (De Beco 2010). The author examines how human rights monitoring can help to improve corruption monitoring, and how it can address human rights violations resulting from corruption acts.

According to this scholar, the definition of *human rights monitoring* is the examination of the occurrence and nature of human rights violations and the identification of the changes that could be brought in order to reduce these violations. This activity, the scholar writes, has the power to create a culture of *transparency* and *openness*, because it makes the public aware of abuses and allows organisations concerned with human rights to make their claims to governments (De Beco 2010: 1108).

Last, but not least, although difficult to achieve, corruption monitoring can contribute to combating corruption and, provided it is sufficiently detailed, it can assist anti-corruption organisations in identifying key problems and in setting priorities, and can also mobilise public support and encourage governments to try and reduce corruption practices (De Beco 2010: 1110).

References

Abu El-Ata, Ahmad, and Monira. 2011. Technology and the Egyptian revolution. http://www.bsgroup.ch/fileadmin/daten/TI/PDF/Publikationen/tim-special11/Einzelartikel/tim11-Society-Ahmad_und_Monira_Aau_El-Ata.pdf. Accessed 25 Oct 2011.

Bowman, Gregory W. 2004. E-mails, servers, and software: U.S. export controls for the modern era. *Georgetown Journal of International Law* 35: 319–378.

Burns, Alex, and Ben Eltham. 2009. Twitter free Iran: An evaluation of twitter's role in public diplomacy and information operations in Iran's 2009 election crisis. http://vuir.vu.edu.au/15230/1/CPRF09BurnsEltham.pdf. Accessed 23 Oct 2011.

Ciobanu, Ceslav. 2010. Lessons of 'velvet revolutions': From Romanian "December 89" to Moldovan "April 09". Moldova: Quo Vadis?. http://cogito.ucdc.ro/sitev/nr_2v2/LESSONS%20OF%20VELVET%20REVOLUTIONS.pdf. Accessed 11 Oct 2011.

Comninos, Alex. 2011. User-generated content and social networking in the Arab spring and beyond. http://www.apc.org/en/system/files/AlexComninos_MobileInternet.pdf. Accessed 24 Oct 2011.

Croeser, Sky. 2009. The global justice movement and struggles over knowledge. http://curtin.academia.edu/SkyCroeser/Papers/111796/Croeser_2009_The_global_justice_movement_and_struggles_over_knowledge. Accessed 25 Oct 2011.

Crosby, Scott, Ian Goldberg, Robert Johnson, Dawn Song, and David Wagner. 2001. A cryptanalysis of the high-bandwidth digital content protection system. http://www.cypherpunks.ca/~iang/pubs/hdcp-drm01.pdf. Accessed 23 Oct 2011.

De Beco, Gauthier. 2010. Monitoring corruption from a human rights perspective. *The International Journal of Human Rights* 15(7): 1107–1124.

Esfandiari, Golnaz. 2010. The twitter devolution. http://www.foreignpolicy.com/articles/2010/06/07/the_twitter_revolution_that_wasnt. Accessed 25 Oct 2011.

Etling, Bruce, Robert Faris, and John Palfrey. 2010. Political change in the digital age: The fragility and promise of online organizing. http://dash.harvard.edu/handle/1/4609956. Accessed 14 Nov 2011.

Eunjung Cha, Ariana. To attacks' toll add a programmer's grief. 2001. http://www.washingtonpost.com/ac2/wp-dyn/A1234-2001Sep20. Accessed 23 Oct 2011.

Fandy, Mamoun. 1999. CyberResistance: Saudi opposition between globalization and localization. *Comparative Studies in Society and History* 41(1): 124–147.

Felten, Ed. 2010. Why did anybody believe Haystack? https://freedom-to-tinker.com/blog/felten/why-did-anybody-believe-haystack. Accessed 25 Oct 2011.

Forte, Maximilian C. 2009. Twitter and the Iranian election protests an annotated bibliography. http://www.openanthropology.org/irantwitterbibliography.pdf. Accessed 23 Oct 2011.

Fuglsang, Lars. 2005. IT and senior citizens: Using the Internet for empowering active citizenship. *Science, Technology, & Human Values* 30(4): 468–495.

Gheblawi, Ghazi. 2011. Libyan re-independence and reclaiming the revolution. http://boell-meo.org/downloads/Perspectives_02-27_Ghazi_Gheblawi.pdf. Accessed 23 Oct 2011.

Giridharadas, Anand. 2010. Africa's gift to silicon valley: How to track a crisis. http://www.nytimes.com/2010/03/14/weekinreview/14giridharadas.html. Accessed 26 Oct 2011.

Goldstein, Joshua, and Juliana Rotich. 2008. Digitally networked technology in Kenya's 2007–2008 post-election crisis. http://cyber.law.harvard.edu/sites/cyber.law.harvard.edu/files/Goldstein&Rotich_Digitally_Networked_Technology_Kenyas_Crisis.pdf.pdf. Accessed 13 Nov 2011.

Hellström, Johan. 2011. Mobile governance: Applications, challenges and scaling-up. In *Mobile technologies for conflict management. Online dispute resolution, governance, participation*, ed. Marta Poblet, 159–179. Dordrecht/Heidelberg/London/New York: Springer.

Hodge, Nathan. 2009. Inside Moldova's twitter revolution. http://www.wired.com/dangerroom/2009/04/inside-moldovas/. Accessed 26 Oct 2011.

Horner, Lisa. 2011. A human rights approach to the mobile internet. http://www.apc.org/en/system/files/LisaHorner_MobileInternet-ONLINE.pdf. Accessed 26 Oct 2011.

Huang, Andrew "bunnie". 2002. Keeping secrets in hardware: The Microsoft XBoxTM case study. http://web.mit.edu/bunnie/www/proj/anatak/AIM-2002-008.pdf. Accessed 23 Oct 2011.

Hudson, John. 2011. The "Twitter Revolution" debate: The Egyptian test case. http://www.theatlanticwire.com/global/2011/01/the-twitter-revolution-debate-the-egyptian-test-case/21296/. Accessed 23 Oct 2011.

Ingram, Mathew. 2011. Was what happened in Tunisia a twitter revolution? http://gigaom.com/2011/01/14/was-what-happened-in-tunisia-a-twitter-revolution/. Accessed 23 Oct 2011.

Jennings, M.Kent, and Vicky Zeitner. 2003. Internet use and civic engagement: A longitudinal analysis. *Public Opinion Quarterly* 67(3): 311–334.
Kabay, M.E. 2010a. Lesson in a Haystack: Kerckhoffs'principle in action. http://www.mekabay.com/nwss/833_lesson_in_a_haystack--kerckhoffs_principle.pdf. Accessed 25 Oct 2011.
Kabay, M.E. 2010b. Lesson in a Haystack: Idealists take on the theocracy. http://www.mekabay.com/nwss/832_lesson_in_a_haystack--idealists_v_theocrats.pdf. Accessed 25 Oct 2011.
Krapp, Peter. 2005. Terror and play, or what was hacktivism? *Grey Room* 21: 70–93.
Ku, Vicky. 2005. A critique of the Digital Millenium Copyright Act's exemption on encryption research: Is the exemption too narrow? http://www.yjolt.org/files/ku-7-YJOLT-465.pdf. Accessed 16 Oct 2011.
Kulesza, Joanna. 2008. Freedom of information in the global information society – The question of the internet bill of rights. *University of Warmia and Mazury in Olsztyn Law Review* 1: 81–95.
La Rue, Frank, and Olof Ehrenkrona. 2010. Chairmen's conclusion of expert meeting on human rights and the Internet. http://www.sweden.gov.se/content/1/c6/13/93/96/829645b7.pdf. Accessed 23 Oct 2011.
Lane, Jill, and Ricardo Dominguez. 2003. Digital Zapatistas. *TDR* 47(2): 129–144.
Litra, Leonid. 2010. The evolution of multi – party system in Moldova in the post – soviet period leonid. http://www.nceeer.org/Programs/Carnegie/Reports/litra.pdf. Accessed 23 Oct 2011.
Mckenzie, Jon, and Rebecca Schneider. 2000. Critical art ensemble tactical media practitioners: An interview. *TDR* 44(4): 136–150.
Miguel, Teresa M. 2011. The digital legal landscape in South America: Government transparency and access to information. http://conference.ifla.org/past/ifla77/194-miguel-en.pdf. Accessed 14 Nov 2011.
Morozov, Evgeny. 2009a. Iran: Downside to the "Twitter Revolution". *Dissent* 56(4): 10–14.
Morozov, Evgeny. 2009b. Moldova's twitter revolution. http://neteffect.foreignpolicy.com/posts/2009/04/07/moldovas_twitter_revolution. Accessed 25 Oct 2011.
Morozov, Evgeny. 2010a. The great internet freedom fraud. http://www.slate.com/articles/technology/technology/2010/09/the_great_internet_freedom_fraud.html. Accessed 25 Oct 2011.
Morozov, Evgeny. 2010b. Hay-what? http://neteffect.foreignpolicy.com/posts/2010/09/02/hay_what. Accessed 25 Oct 2010.
Mungiu-Pippidi, Alina, and Igor Munteanu. 2009. Moldova's "Twitter Revolution". *Journal of Democracy* 20(3): 136–142.
Munöz, Lucia Liste, and Indra de Soysa. 2011. The blog versus big brother: New and old information technology and political repression, 1980–2006. *The International Journal of Human Rights* 15(8): 1315–1330.
Pfister, Damien Smith. 2011. The logos of the blogosphere: Flooding the zone, invention, and attention in the Lott Imbroglio. Argumentation and Advocacy 47(3). http://vlex.com/vid/logos-blogosphere-flooding-lott-imbroglio-311259242. Accessed 11 Nov 2011.
Russell, Adrienne. 2005. Editorial: Exploring digital resistance. *New Media & Society* 7: 513–515.
Sambidge, A. 2012. Rights group slams Kuwaiti's Twitter sentence. http://www.arabianbusiness.com/rights-group-slams-kuwaiti-s-twitter-sentence-461416.html. Accessed 10 June 2012.
Sampaio, Lucas. 2012. Facebook bloqueia usuárias que aparecem seminuas em fotos da Marcha das Vadias. http://www1.folha.uol.com.br/tec/1097488-facebook-bloqueia-usuarias-que-aparecem-seminuas-em-fotos-da-marcha-das-vadias.shtml. Accessed 10 June 2012.
Samuelson, Pamela. 2001. Anticircumvention rules: Threat to science. *Science* 293(5537): 2028–2031.
Sartor, Giovanni. 2010. Human rights and the future of the information society.http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1707724. Accessed 25 Oct 2011.
Shalhoub-Kevorkian, Nadera. 2011. E-resistance among Palestinian Women: Coping in conflict-ridden areas. *The Social Service Review* 85(2): 179–204.
Sohrabi-Haghighat, M. Hadi, and Shohre Mansouri. 2010. 'Where is my vote'. ICT politics in the aftermath of Iran's presidential election. http://www.swinburne.edu.au/hosting/ijets/journal/V8N1/pdf/Article2Sohrabi&Mansouri.pdf. Accessed 25 Oct 2011.

Solop, Frederic I. 2001. Digital democracy comes of age: Internet voting and the 2000 Arizona democratic primary election. *Political Science and Politics* 34(2): 289–293.

Sunstein, Cass R. 2010. Open government and records management. http://www.archives.gov/records-mgmt/pdf/sunstein-raco2010.pdf. Accessed 1 Nov 2010.

Tismaneanu, Vladimir. 2009. Moldova's revolution against cynical and cronyist authoritarianism. http://www.rferl.org/content/Moldovas_Revolution_Against_Authoritarianism/1607656.html. Accessed 22 Oct 2011.

Virak, Ou. 2011. Internet censorship: The ongoing crackdown on freedom of expression in Cambodia. http://www.ifex.org/cambodia/2011/06/20/internet_censorship.pdf. Accessed 7 Nov 2011.

Wellman, Barry, and Xiaolin Zhuo. 2010. Egypt: The first Internet revolt? http://homes.chass.utoronto.ca/~wellman/publications/egypt/PMag-1107-Egypt-offprint.pdf. Accessed 23 Oct 2011.

Whitty, Noel. 2010. Soldier photography of detainee abuse in Iraq: Digital technology, human rights and the death of Baha Mousa. *Human Rights Law Review* 10(4): 689–714.

Wu, Min, Scott A. Craver, Edward W. Felten, and Bede Liu. 2002. Analysis of attacks on SDMI audio watermarks. http://www.ece.umd.edu/~minwu/public_paper/icassp01_sdmi.pdf. Accessed 23 Oct 2011.

Yen, Alfred C. 2003. What federal gun control can teach us about the DMCA's anti-trafficking provisions. http://www.chicagoip.com/yenarticle.pdf. Accessed 23 Oct 2011.

York, Jillian C. 2010. Haystack and media irresponsibility. http://jilliancyork.com/2010/09/13/haystack-and-media-irresponsibility/. Accessed 25 Oct 2011.

Zimmermann, Philip. 2001. No regrets about developing PGP. http://www.philzimmermann.com/EN/essays/index.html. Accessed 23 Oct 2011.

Zhuo, Xiaolin, Barry Wellman, and Justine Yu. 2010. Egypt: The first internet revolt? *International Journal of Emerging Technologies and Society* 8(1): 24–41. http://homes.chass.utoronto.ca/~wellman/publications/egypt/PMag-1107-Egypt-offprint.pdf. Accessed 21 November 2011.

Zuckerman, Ethan. 2011. The first twitter revolution? Not so fast. The internet can take some credit for toppling Tunisia's government, but not all of it. http://www.foreignpolicy.com/articles/2011/01/14/the_first_twitter_revolution. Accessed 25 Oct 2011.

Chapter 3
Hacking and Digital Dissidence Activities

3.1 The Role of Hackers in the Landscape of Digital Resistance

In this framework of the right to digital liberties, hacking may take on an equally important role: that of contrasting the process of *closure* that threatens to exclude future generations from fully enjoying their vast heritage, consisting of both culture and liberties, but both, however, are also increasingly compressed and stifled. At this point in time, it appears that we are completely uninterested in the future, and in the liberties, digital and otherwise, that we will leave to our children.

Lawrence Lessig's remarks with regard this issue, outlined in the preface of his book *Remix*, on the "copyright wars" and their influence on future generations, are quite insightful:

> […] I don't doubt the concerns I had about innovation, creativity, and freedom. But they don't keep me awake anymore. Now I worry about the effect this war is having upon our kids. What is this war doing to them? Whom is it making them? How is it changing how they think about normal, right-thinking behavior? What does it mean to a society when a whole generation is raised as criminals? […] In a world in which technology begs all of us to create and spread creative work differently from how it was created and spread before, what kind of moral platform will sustain our kids, when their ordinary behavior is deemed criminal? […] What should we do if this war against "piracy" as we currently conceive of it cannot be won? What should we do if we know that the future will be one where our kids, and their kids, will use a digital network to access whatever content they want whenever they want it? What should we do if we know that the future is one where perfect control over the distribution of "copies" simply will not exist? In that world, should we continue our ritual sacrifice of some kid caught downloading content? Should we continue the expulsions from universities? The threat of multimillion-dollar civil judgments? Should we increase the vigor with which we wage war against these "terrorists"? Should we sacrifice ten or a hundred to a federal prison (for their actions under current law are felonies), so that others learn to stop what today they do with ever-increasing frequency? In my view, the solution to an unwinnable war is not to wage war more vigorously. At least when the war is

G. Ziccardi, *Resistance, Liberation Technology and Human Rights in the Digital Age*, Law, Governance and Technology Series 7,
DOI 10.1007/978-94-007-5276-4_3, © Springer Netherlands 2013

> not about survival, the solution to an unwinnable war is to sue for peace, and then to find ways to achieve without war the ends that the war sought. Criminalizing an entire generation is too high a price to pay for almost any end. It is certainly too high a price to pay for a copyright system crafted more than a generation ago (Lessig 2009: xvii–xviii).

We are *closing* rather than *opening*; castigating rather than de-penalizing behaviors which are not only made possible by the diffusion of new technologies but by now are also so completely common that they can no longer be perceived as illicit; we are choosing to abandon fundamental rights, first and foremost our privacy and freedom of speech, in exchange for an erroneous faith in the idea that these compromises might somehow lead to greater security or to the protection of a few limited privileges that are in all likelihood destined, sooner or later, to be swept away by the tidal wave that is Internet.

Technology, today, offers the greatest possibility ever afforded to mankind to fully express and enjoy our fundamental human rights. At the same time, however, all nations, none excluded, are actively seeking to stem this tide, without comprehending that it is simply impossible to do so.

The aims of the hackers of 50 years ago have been, in many aspects, fully met. Anyone, today, utilizing technology correctly, can unlock systems perceived to be unjust, can circumvent oppressive laws, can protect their personal privacy, their freedom of speech and anonymity, and can contribute to making public administrations increasingly transparent (despite claims to the contrary, it is this last element that is most feared by the political classes of every nation).

Unfortunately, this possibility for us to individually assert our digital rights and liberties is, in many cases, considerably compromised when our own governments actively oppose it.

3.2 A First Analysis of Common Threats to Digital Freedom and to Hacker Activities

An analysis, in fact, of those countries in which technology is perceived as a threat, and in which the possibility of the full exercise of digital rights is perceived as a negative rather than a positive element, reveals a portrait that is significant indeed. The *OpenNet Initiative*, in collaboration with activists from *Amnesty International* and *Reporters Sans Frontières*, keeps, *inter alia*, close watch on the state (or rather, on the "level") of technological freedoms throughout the world, paying constant attention to those actions which limit the exercise of digital liberties.

The most common actions designed to prevent individuals from fully enjoying their right to liberties in the electronic world are, essentially, four:

1. the action of content filtering;
2. the action of censoring;
3. generalized and indiscriminate surveillance; and
4. the arrest of those perceived as digital dissidents.

The four most common motivations that compel dozens of states throughout the world to justify more or less stringent forms of global surveillance, censorship and even violent intervention against digital rebels are:

1. the protection of intellectual property rights;
2. reasons of national security;
3. the need to preserve local cultural norms and religious values; and
4. the protection of children from pornographic material and entrapment by pornographers.

At the basis there is, in all nations, the conviction that it is necessary to intervene decisively because of the existence of a *medium*, Internet, that is not sufficiently regulated: there are not, according to this view, enough *specific* laws. But even this is simply another excuse: more laws related to Internet have been passed over the last few years than ever before, and persisting in maintaining that Internet is a legal no man's land[1] is, by now, an affirmation that is not only false, but anachronistic as well.

John Perry Barlow, in his prescient article *Censorship 2000*,[2] noted that entities who resort to censorship and to limiting the rights of Internet users, who "*aspire to edit collective human consciousness*" and to horde power, can be divided into diverse categories: nation-states, local governments, corporations, religious entities, cultural groups, one-to-many content providers and individual information owners (Barlow 2000).

According to Barlow, the typical pretexts used to justify such actions are varied. Frequently utilized is the protection of children from exposure of sexually explicit or violent materials, or the prevention of the entrapment of minors for exploitation in the production of child pornography, used often as a justification to ban its distribution.

Other typical excuses are the political suppression of groups considered marginal (whether neo-nazi groups in Germany, or women in Saudi Arabia), the need to defend national or commercial security (by preventing the distribution of software

[1] See the interesting McLure's essay concerning the ways in which the electronic frontier builds upon the mythology of frontier expansion generally, and the western American frontier in particular (McLure 2000). The author notes that "Like the western frontier, the e-frontier is vitally significant to American economic and strategic interests that were manifested first in continental (and now wired) expansion; yet the cyberfrontier also appeals on a popular level to many romantic, nostalgic western myths about endless horizons, unlimited opportunity, and untrammeled freedom" (McLure 2000: 458). More: "The cowboy/rebel/outlaw of the electronic frontier is, of course, the hacker, already a somewhat mythical figure in the American collective imagination and able to perform technological feats and engage in criminal activities in a digital territory that most Americans will never even see, let alone traverse. Like the real cowboy of the Old West, hackers maybe regarded with both disdain and admiration. They are also usually very young, technically proficient men, and they employ their own specialized jargonor lingo. But they bear much more resemblance to the counterculture antiheroes of Western films of the late 1960s and 1970s than they do to traditional cowboy heroes like the Virginian or Hopalong Cassidy" (McLure 2000: 462).

[2] See http://www.isoc.org/oti/articles/1000/barlow.html. Accessed 14 November 2011.

for encryption, decryption and hacking) or to protect governments, corporations and religious groups from destabilizing, inflammatory, or embarrassing expressions by dissidents or internal whistleblowers.

Also common are tactics aimed at limiting the exposure of a certain culture to the expressions of another culture deemed, for whatever reason, to be offensive, seeking to disarm terrorists by preventing online distribution of information about explosives or weapons, reducing the flow and consumption of illegal drugs by banning information regarding their production or by banning positive statements about their effects.

Another much used justification for censorship is the proclaimed "urgent need" to prevent communication between criminals, terrorists and drug traffickers, to protect governments and corporations from revelations of industrial or state secrets, to protect individual privacy by regulating the exchange of personal information, to restrict transmission of unsolicited materials (spam), and, ever more frequently, to prevent the noncommercial distribution of copyrighted materials.

But Barlow's conclusions are optimistics:

> Ultimately, I'm optimistic. I have believed, since I first came upon the Internet, that one day it would enable any people, anywhere, to express whatever they wished-distributing their expressions to all who were interested and ensuring their posterity-without fear of punishment or censure. I have believed that the Internet promises humanity more freedom of expression than we have ever experienced and that the fruits of that freedom will transform our species into one great and God-like Mind. I have realistic hope for a future in which economic productivity is vastly amplified by knowledge, in which inequities in distribution are leveled, and in which the meek might outthink the mighty. I still believe in that future despite all of the efforts to forestall it that I've touched on here. I believe in it because I believe that the ripe force of unconstrained creativity is already working on methods to preserve itself. Even though Napster will probably be crushed, there are already new methods for storing and sharing proscribed materials, such as Gnutella and Freenet, that have no centralized servers or legally vulnerable entities to shut down. Moreover, there are already data havens springing up where rogue governments are defying the G8 and allowing servers within their boundaries to contain any information the users wish to place on it. Mostly, I believe in that future because I fully expect most of the human species to have Internet access within the next decade. Once that has happened, the Party of the Past will lose its currently unwired constituencies, and there will be few left who believe the excuses it still uses to mute the human spirit. Indeed, I believe that eventually the truth really will set us free (Barlow 2000).

3.3 Being a Hacker in This Framework

3.3.1 Thinking Like a Hacker

What sense could there be, today, in our increasingly connected (and increasingly observed) society, for average users and common citizens to commit to taking up the hacker way, in the constructive sense (and *not* in the destructive or criminal sense) described above? What good could ever come from having studied these phenomena from a new standpoint, with the objective of using them as the basis for new

action? What importance could there ever be in handing down to future generations such ideas and an approach to technology which, despite the passing of years and decades, is still not only at the forefront, but also ideal for bringing about undoubtedly positive change?

And above all, what good could possibly come from a highly developed understanding of currently available technology, from the point of view of the possibility of *hacking the system*, understood as the political, economic, and social system, the media apparatus, the world of art and literature, the universe of computer code and culture?

Taking inspiration from the classification first presented by Mike Godwin in his book *Cyber Rights*: *defending free speech in the digital world*, three principal objectives for electronic resistance may be identified as follows (Godwin 1998):

1. hold the steadily growing government powers to intervene in the lives of individuals to precise *boundaries* and *constitutional limits*;
2. oppose decisions and political strategies regarding Internet that are plainly based on backlash and fear of technology, and not on the well-being of individuals, society, the economy and the overall efficiency of the system;
3. demand from the state *unconditional respect* for its citizens and for the power that they may wield through the use of computers and the Internet.

In a political environment such as ours today, returning *tout court*, without any critical sense, to the concepts at the basis of hacking, its origins and its old school of thought, and seeking to apply those concepts to this decade's social realities, does not, in all probability, make much sense.

There have been too many changes, not only to the overall context, but especially in terms of the current political fabric. But above all, over the course of the last 20 years, the "technological revolution" has had too strong an impact, and has changed the very fundamentals of so many aspects of our lives.

It might be more effective, instead, to consider how those "old principles" might take on new forms and a renewed, invigorated potential, resulting from the delicate interpretation made possible by the myriad new possibilities which technology has now placed into all of our collective hands.

One first fact to bear in mind is that "old school" hackers began, in a certain sense, with a disadvantage, as compared to hackers of our age.

Their machines were slow, difficult to use, and simply understanding them, much less using them, took up an enormous amount of time for early computer users.

Certainly these challenges increased their abilities, but with those first machines, remarkable outcomes were few and far between and did not come without weeks of work and countless sleepless nights. Some renowned hackers from the early periods spent days travelling from one state to another simply to find a particular manual or technical document.

Today even teenagers have their own computers, and, above all, access, if they wish to seek it out, to a network of know-how and a set of information which allow any of us to achieve within seconds, seamlessly and without any particular effort,

results that would have been unthinkable in those early years. This was actually the aim and aspiration of the cited activist Lee Felsenstein, and of all those rebels who fought, during the 1970s, for the dream of "a computer for all", in every home, in every neighborhood, in every park, in every library.[3] They worked toward this aim because they were certain that increased access to computers would lead to a better society, to a democracy that, if not perfect, would be at least more transparent, and, more than anything else, because they believed that it would lead not only to an improved relationship between the state and its citizens, but even to an increasing distribution and circulation of culture.

This first point merits further consideration.

It is hardly a coincidence that many nations, despite countless public statements, un-kept promises, state-publicity and propaganda, have never managed to implement serious incentive policies for either the diffusion of computers amongst their citizens or, above all, of web access points, most especially Wi-Fi hotspots.

It is certainly not a coincidence that many countries have never provided for ministries, or similar government departments, dedicated expressly to technology and to development of the computer sciences within their countries, to the creation of "an electronic backbone", of a telematics nervous system accessible to all.

Many ask why, in self-proclaimed advanced countries, there is no nationwide free access to the Internet, frequently absent not only in metropolitan areas but most especially in more rural, disadvantaged areas.

Already by the 1970s, a number of illuminated theoreticians were proposing that the first step would be to connect everybody. *Connect*. From that moment, and only from that moment, would it be possible to consider the computer as conceivably beneficial for humanity.

Consider my country, Italy: despite the fact that, since the 1990s, countless governments have announced the impending creation of a single digital network, uniting public offices, courts, and central and local administration, in most sectors everything has remained exactly as it has always been, in terms of efficiency or, rather, the lack thereof. The conclusion is that in Italy, but also in several other countries, citizens who desire unlimited, free web connections without going to particular bureaucratic and technological effort, except for certain connections guaranteed by municipal network projects or by free networks created by voluntary associations or computer geeks, will be thwarted indefinitely. They will continue to be frustrated, in Italy certainly, because there are so few public access points, and because the few existing public access points are slow and bureaucratized, by law require photo identification and registration, and often involve waiting periods in order to receive an activation code. Only in 2010, fully 5 years after the approval of the anti-terrorism law that established the above constraints,[4] did the Parliament in Rome

[3] See Sect. 1.1.

[4] I am referring to the provisions of the Italian Law n. 155 of 31 July 2005 ("Urgent measures to contrast international terrorism"). See the complete text at the address http://www.camera.it/parlam/leggi/05155l.htm. Accessed 24 November 2011.

propose a bill[5] providing for the elimination of limits to accessing the Internet from public networks.

For many who seek to begin electronic resistance activities, and this is true not just in Italy, but in many countries worldwide, the impression is that of operating in a state which voluntarily keeps its citizens *away* from technology, which is afraid of *computers* (and Internet connections) *for all* because it knows that this would be an important step – an essential step – toward the process of annulling years of caste privileges, partisan handouts, and other systems equally damaging to the well-being of the country's political system.

The problem is due not only to an aging political class that is completely ignorant, from a technical point of view (and not afraid of publically admitting it, and this is especially true of Italy), but is due also to the conviction, held by many leading politicians, that information should be *controlled*.

3.3.2 State Antagonism, Fear and Violence

Thus the worst evil, with regard to Internet policy, is ignorance, as Mike Godwin wrote in 1994 in his illuminating *Cyber Rights*, with reference to the situation in those years in his own country.

According to Godwin, there were three main causes of the antagonism, fear and violence toward the web on the part of both the government and the political world in general (Godwin 1998):

1. a reaction against the excessive visibility of Internet;
2. the voluntary desire to create hate and fear of the web for ulterior purposes, and the evident ignorance of the nature of the web, of the principles that could be applied and its original characteristics; and
3. the knowledge that the opening of the digital world to a country's citizens might well become an arm of unprecedented strength in their hands.

From Godwin's logical and lucid observations one can derive, reasoning in reverse, the most salient and compelling motives for opposition today, in the present: the state is *afraid* of Internet, therefore it will never legislate rationally, but always with an eye to controlling it and repressing it; the political classes, barring a certain number of rare exceptions, have little or no understanding of the web's potential, its technologies, its traditions and behaviors, and therefore will never be

[5] I am referring to the draft bill related to the Law Decree n. 187 of 12 November 2010 ("Urgent measures regarding security issues"). See the complete text at the address http://www.interno.it/mininterno/export/sites/default/it/sezioni/servizi/legislazione/sicurezza/0965_2010_11_12_DL12112010n187.html. Accessed 24 November 2011.

able to operate correctly; states do not want to open technology to their citizens because they are afraid of losing privilege and power.

To the state's evident inability to provide for the right to free and unfettered access to the Internet – an inability, as mentioned above, that in many cases leaves the observer unsure as to whether it originates from mere incompetence and ignorance on the part of those entrusted with the creation of this system, from administrations based on partisan politics and handouts and less than transparent state bidding systems which together create an environment in which this instrument could never function at all, or, on the other hand, due to a real fear of consolidating too much power in the hands of the citizens.

There is, however, a new, positive phenomenon, a factor which is perfectly capable of minimizing this technological strong-arming by state, typical of even nations considering themselves civil: today many individuals possess a cellular phone and a computer. Possessed out and out, not provided by the state, they are connected to commercial Internet providers, especially in homes.

They are expensive, certainly: data and telephone fees are still quite high. Many, however, are beginning to realize that, in fact they are, albeit perhaps unexpectedly, perfectly equipped to hack the system, to get around a failing technical policy, to evade unfair and oppressive laws, to carry out digital objection activities, to take transparency and new, digital eyes into areas and procedures that the public sector would rather remained covered under a veil of (state) secrecy.

Common citizens today have in their hands, in their pockets, in their backpacks and in their handbags the most powerful instrument ever invented to protect free speech, to act in effective anonymity, to guarantee the confidentiality of our personal data, to focus attention on any faults in the security of large-scale public sector computer projects, to guarantee the free circulation of information on a scale and with an effectiveness never before even imaginable.

They have in their hands the tools to inspire the rethinking of concepts of publication bans and censorship, secrecy, wiretaps, intellectual property, the free circulation of knowledge and culture.

It is as though in the place of a state computer policy, which will never be fully realized due to the evidently ever present fear of putting too much power into the hands of citizens, there were a new "citizen's computer policy", a network, still fragmented, uneven, and disunited, but nonetheless fundamentally important, which allows citizens to establish contact in real time and to organize for the resolution of not only personal, but increasingly also institutional problems as well.

It is no coincidence that two of today's catchwords, both on the web and off, are *citizen journalism* and *personal democracy*: it would appear that, in this particular historical period, a number of powers that have traditionally been reserved for political and social castes and unapproachable centers of power are now coalescing into the hands of the people.

So, today, especially today, does it still make any sense to be a hacker? Does it make any sense, today, to follow in the footsteps of those first hackers, moving from the basic principles of those early masters and reinterpreting them, at a time in which the curiosity and the sense of challenge which inspired scholars of the past

would now need to be somehow reinvented, and then directed towards a society that is, however, already highly computerized?

Today being a hacker can be not only easier, but, at the same time, more efficient than in the past. Easier, given that hackers, in the past, had exceptional minds (and had to, as the technology available to them presented challenges that could only be resolved with dedication and reasoning skills far beyond normal capacities), but had very little information to work with; they did not have a world library on hand to satisfy every question they had at the touch of a mouse.

The ease of use of today's technology, and the far greater diffusion of technical information, can save time and allow quick thinking hackers to reach greater objectives with less intellectual effort.

Their thirst for culture can be satisfied in seconds. It is as though this enormous flow of information were creating difficulties for those countries and those situations that sought strength in the controlling, parceling out, and obscuring of information, that sought to keep their citizens and subjects in ignorance in order to prevent that different, freer information, or simply information of a different nature, might awaken a critical sense within their borders.

Moreover, being a hacker, today, is often more efficient than in the past for yet another reason: every individual may become a part of a larger system that seeks to oppose the *status quo*, using the tools offered by the digital world.

While it is true that hackers of the 1960s and 1970s could count on "primitive" webs, but there is no comparison to today's capacities for disseminating, circulating and diffusing information.

This has led, and this is not a hyperbole, to an exponential increase in transparency that is unprecedented in the history of mankind.

Today we can pass from local to global in an instant. Our voices can be heard by millions of people at the push of a button, our writings read in all four corners of the world in seconds, at any moment we can meet other individuals with similar interests, ready to unite for common action.

If in the past, and, for example, in the grand constitutional tradition of the United States, the press was acknowledged to be the watchdog of democracy, today we have reached a point in which that role of watchdog may be carried out to perfection by technology, guided by humans.

3.4 A Brand New Playground

3.4.1 Liberation Technologies

A number of American scholars have, for some time, held discussions regarding a set of new *liberation technologies*. In determined events and political situations, the web's unique abilities to empower the individual, to facilitate independent communication, to mobilize, to reinforce an emerging civil society and to further the cause

of liberty appear to be unsurpassed. Liberation technologies permit individuals to report on news events, render public misdeeds, express opinions, mobilize protests, monitor elections, analyze the activities of government, increase participation[6] at all levels and to expand the horizons of liberty. These abilities are, obviously, contrasted by states which have, in turn, invested time and resources on actions aiming to obtain precisely the opposite effect, with technologies for censorship and surveillance, and with the growing capacity to identify and punish any and all dissenters.

There is a sort of "race for technology" on both sides, but with dramatically differing objectives. And it is this factor, this fundamental, paradoxical dichotomy, which is perhaps the most intriguing aspect of the environment surrounding digital resistance today.

Adopting a general categorization, created in the United States, incorporated by the *Electronic Frontier Foundation* (EFF) (in all likelihood today's most important group working for the defense of rights in the digital world) into the very structure of their web site, and taken up by the majority of activist associations throughout the world, the five principal fields of action typical of digital resistance can be seen as:

1. the defense of free speech;
2. the protection of innovation and progress in the social fabric;
3. the reform of intellectual property laws in order to adapt them to technological progress;
4. the protection of privacy;
5. the pursuit of transparency.

Within these five macro-fields of action, it is possible to identify a number of subcategories which allow hackers, or anybody who desires to take action to improve the state of things, a wide margin of functionality even in very specific and narrow settings (and which may be "surgically" adapted to fit action to local political contexts).

[6] Concerning the effects of the Internet on political participation, see the essay by Tolbert and McNeal (Tolbert and McNeal 2003). According to these scholars: " […] there is also evidence to suggest that changes in communication technology may play an important role in influencing electoral behavior" (Tolbert and McNeal 2003: 175). Conclusions are clear: "While not a panacea for the disenfranchised, the Internet may nevertheless represent an important new venue for political information and communication, and counter declining civic engagement in America. It also raises broader questions about democratic participation" (Tolbert and McNeal 2003: 184). See also the study by Zavestoski, Shulman and Schlosberg regarding democracy and the environment on the Internet, and electronic citizen participation in regulatory rulemaking (Zavestoski et al. 2006). The authors notes that: "Although the Internet has the potential to facilitate deliberative processes that could result in more widespread public involvement, greater transparency in government processes, and a more satisfied citizenry, […] efforts to implement Internet-based public participation have overlaid existing problematic government processes without fully harnessing the transformative power of information technologies". (Zavestoski et al. 2006: 383). They note, also, that "In theory, the Internet provides novel capacities for reflexive decision making on a national scale. An open, Web-based process has the potential to help move environmental policy making beyond the adversarial distrust, the battles over science, and the state's predisposition against public values" (Zavestoski et al. 2006: 404).

A similar classification was created in the United States over 20 years ago: it is naturally based on standards developed there; however, it is, in any case, useful in any country for the creation of precise plans of action and a sort of preliminary "plan of operations".

The first class of action, the protection and safeguarding of free thought, is probably the most important and the largest, but, above all, it is that which denotes our technical society, laying the ground for truly bitter conflicts.

As is clearly indicated on EFF's web site, many activities carried out by activists, from the daily use of e-mail and social networking site to updating blogs and web sites are essentially forms of diffusion of information. Internet is radically changing the way we "create" information, from the ways it is accessed to how, where and when it is divulged, and this last is, increasingly, in the hands of simple web users. Added to this, is the possibility, fundamental as it is now concrete, of *sharing ideas* and content with users, in real time, throughout the world. At the same time, however, in this same framework can be found, in many parts of the world, of the same fundamental importance and just as concrete, more or less covert attempts on the part of national governments or private enterprises to seek to limit or control the constant, worldwide conversation created, facilitated and sustained by the Internet.

Activists, today, are well aware that there are two necessary factors needed each day to preserve a minimum of liberty and freedom on the web: protecting the web's open architecture, and never, ever forgetting a simple fact: that a technology, even the freest and most neutral of technologies, can amount to nothing if it is not supported by a legal system that *protects* it.

Thus if the same legal system that is to protect digital technologies is the first to censure them, or to limit access to determined information, or restrict the use of communication tools, the potential of the Internet may never be fulfilled.

Internet has become, in the modern age, the most important platform for the exercise of free speech; every time an activist "moves" online to express himself or herself in the digital world, his or her right for the freedom of expression and the freedom of thought should, and must be, respected in the digital domain just as they are respected and protected by countless constitutions and bodies of law throughout the world.

In the United States alone it is by now nearly impossible to list the myriad of cases involving online free speech which have spurred digital activists to action.

One of the "classic" cases, which reached the Supreme Court, involved the CDA (*Communications Decency Act*), approved by Congress and signed into law by President Clinton, which sought to protect minors by indiscriminately blocking completely legitimate content. The CDA was followed by the COPA (*Child Online Protection Act*), which established penal sanctions for the online distribution of material deemed potentially dangerous for minors. Over the last 15 years, in North American these and other similar measures have generated heated debate with regard to their constitutionality; numerous issues have been raised, ranging from the unclear wording of such provisions to the consequential reductions in freely accessible materials such measures engendered (thereby involving the issue of free speech), to patent symptoms of censorship, violation of the privacy of adult users and the unjustified restriction of the right to divulge information on the web.

At the base of it all was the clear intention to "make the web decent" and to define standards for the digital world, an attempt which fortunately (for now) has not (yet) been entirely successful but which has created serious concern worldwide given that it originated in the United States, recognized by all to be fundamentally important, but that at the same time is not necessarily a progressive context (in fact, especially where Internet is concerned, thought in the United States can be quite conservative).

Three activist associations, EFF, ACLU and EPIC, have all, since the introduction of these restrictive measures, fought, with a considerable degree of success, to have them declared unconstitutional. Today they continue to monitor United States politics and policy regarding these issues, as the politicians in Washington DC continue to introduce new similarly restrictive bills at regular intervals.

In other cases (for example the EFF's *No Downtime for Free Speech Campaign*), activists have worked to establish the concrete connection between the ability of an individual to cite a portion of copyrighted protected works for the purposes of self expression, the deluge of cease-and-desist letters these activities often produce and the protection of free speech.

This interpretation might appear complex, but in reality it is quite linear. Think about how often we come across personal blogs quoting the work of others, news sites containing clips from relevant television programs, or even online parodies based on fragments of pop songs: in all of these cases, a cease and desist letter (an order or request to halt an activity or remove certain materials facing legal action) from the entities holding the copyrights to those works cited clearly has intimidating and repressive effects. Even in those cases in which, from a strictly legal point of view, the use of a portion of the work cited would in fact be legitimate (and, therefore, in the event of a trial, the individual responsible for having put the excerpts in question online would not risk sanctions) the mere intimation of legal action of any kind is enough, in the vast majority of cases, to spur the speedy removal of the materials, in order to avoid even the risk of legal proceedings.

EFF has clearly documented that, in the United States, thousands of such letters are sent each day, addressed to both individuals and Internet providers, and that this continually expanding "web" of intimations has had a concretely censoring effect, even in cases of the citation of works which the law would deem perfectly legitimate. This problem has been raised in Italy as well, in cases in which certain blogs, or sites featuring political information, were threatened with legal action or claims for damages amounting to millions of euros due to the opinions they contained. The threat of legal action, or even a traditional warning letter, even if different from the American cease-and-desist letters, in Italy has been enormously effective in obtaining the same results.

3.4.2 Anonymity and Bloggers' Rights

Within the general and fundamentally important category of free speech there are, as mentioned above, a number of sub-categories that are of no less importance: I am referring, in particular, to the protection of anonymity and to the rights of bloggers.

With regard to the former, it is manifest that many individuals do not wish, for any number of reasons, that their online writings have any connection to their real identities and their offline personas. They may fear, for example, political retaliation, dismissal from work, or even violence or threats to their very lives.

In the United States, the Supreme Court has been inclined, in a number of decisions, to recognize that anonymous speech does in fact fall under the right to free speech and that, as such, must be protected, given that this right is vital for democracy and is a shield against the "tyranny of the majority" (especially in regard to more unpopular positions).

Online protection of anonymity in the real world is important as well, given that the Internet offers a new and dynamic forum for discussion. In fact, the web's unique capacity to spread information, and in this way to further promote democracy, is in many cases guaranteed precisely by the possibility the digital world affords to communicate anonymously.

That is why another EFF project, *CyberSLAPP*, works toward the goal of protecting those who seek web anonymity. The rights of bloggers obviously raise evident free speech issues: bloggers have faced considerable legal intimidation and threats of legal action due not only to their own writings but due also to the comments their work may generate.

The relationship with journalism, the protection afforded to that sector, especially in countries with strong traditions in this sense, the right to engage in even heated political expression, the right to remain anonymous and the limitation of liability for bloggers are at this particular juncture, to say the very least, immensely timely topics. In Italy, on the other hand, the only bill advanced in Parliament that in any way addressed Internet anonymity came, somewhat paradoxically, from precisely the opposite perspective: the complete elimination of Internet anonymity in order, ostensibly, to safeguard legality.[7]

The second area of action for digital resistance, no less important than the defense of the freedom of speech on the digital frontier, is the protection of innovation. The pathway toward innovation has always encountered numerous obstacles; in the digital world, threats to further innovation can come from both state regulation and from private enterprise. Sadly, the results are often unambiguous, damaging limitations to liberty, creativity, and competition.

It is particularly interesting, for example, to examine issues regarding the disabled, who battle constantly for accessibility to current technology, and who are at times forced to go to considerable extra effort to evade "protective measures" which do little more, in their case, than to further limit functionality for a group whose functionality is already challenged.

The situation, in such cases, is somewhat paradoxical (and more than a bit sad): new technologies that would significantly improve the lives and learning capabilities of those with difficulties, but the enormous potential is rarely fully exploited, and, to the contrary, technology at times does little more than to increase the challenges they face. Many activists maintain that it is, above all, the disabled who have the

[7] See Sect. 1.3.

clearest right to hack, to alter technologies and legitimately purchased products in order to convert them into tools that are truly useful for their needs. Furthermore, in this perspective, there is a further right, even in the case of copyright protected works, to share those hacks with the rest of the community.

3.4.3 Innovation

With regard to innovation, the EFF *Coders' Rights* project seeks to intervene in yet another extremely important area, held dear to both hackers and activists: the programming of "dangerous" code or the hacking of delicate technologies.

Let me explain: at the base of this type of activism there is the awareness that the programmers and developers involved in advanced exploration of the limits of technology (for example, researchers operating in the fields of security and cryptography) are at a higher risk for legal actions and threats.

Such reactions (which, as mentioned above, generally take the form of cease-and-desist letters and orders) are seen, in this view, as having the capacity to prevent or even inhibit scientific discoveries that might potentially be of enormous use to humanity. Thus this particular EFF project seeks increase awareness of rights and limits, in addition to providing a constant stream of information regarding "hot" topics (and facing the risk of law suits themselves) such as, for example, reverse engineering, vulnerability reporting, and all hacking activities in the "grey zone" that might accidentally, and purely inadvertently, violate the law.

Yet another spiny question is that of DRM technologies, which raises a number of both technical and legal questions. Being, as they are, technologies that essentially control what a user can or cannot do with legitimately purchased products, it is natural that they are particularly exposed to hackers' attentions.

Ed Felten of Princeton University is a scholar whose theories espouse a sort of "right to act", or to breach such systems, in the name of the more important right to knowledge and in order to adapt legitimately acquired products to the needs of their owners. E-books, DVDs, Blu-Ray disks and videogames are four categories which currently attract the activities of hackers, who are convinced that the DRM systems incorporated into these products are designed to suffocate freedom and innovation, without having any effect whatsoever in combatting digital piracy. In addition to these more visible DRMs there are others, just as restrictive but significantly more treacherous: systems to alter the neutrality of the web incorporated into data packets or in servers which send them on to their users, copyright verification initiatives known as *trusted computing*, which actually redesigns personal computer hardware to attach a control system to the computer's mother board.

3.4.4 Intellectual Property and Privacy

A third category which currently provides much fertile terrain for digital resistance activities is the protection of intellectual property. Here, hackers' principal objectives

are copy protection systems, the creation of programs to bypass restrictions on copying, the most efficient distribution of information and works, whether protected or not, on the web, and the protection of the rights of consumers, creators, innovators and scholars.

Probably the most well-known episodes in this regard have been the thousands of lawsuits brought by the *Recording Industry Association of America* (RIAA) against the fans of musical groups and musicians who download songs on peer-to-peer sites. Fairly recently, in 2005, the MGM case against Grokster created a furor and reached the Supreme Court, when 28 of the world's major entertainment companies took successful legal action against the creators of *Morpheus*, *Grokster* and *Kazaa*, software programs with similar functions (and aims).

The fourth battleground, regarding privacy, involves a number of issues that are particularly compelling because they touch upon the most intimate aspects of our lives as human beings.

It is clear that new technologies are leading to further development of individual rights and liberties, but, at the same time, these same technologies also permit an invasion of the private sphere that is without precedent. From mobile phones which allow us to be tracked to the visibility of the terms we look up on search engines, which perhaps contrary to popular opinion are in fact far from secret, privacy in the digital world must in any case be respected, and, what is more, must also be delicately balanced with other individual rights.

These case often bring into play two closely related issues: on the one hand, the extension of rights relating to the protection of personal data in the online world, and on the other, the concrete safeguarding of confidentiality.

The questions surrounding locational privacy are rapidly intensifying, motivated by the fact that individuals increasingly possess instruments which are able to communicate their positions. Not only our mobile phones and now even our iPods and iPads but also our GPS navigators can readily reveal our whereabouts (and that of our cars).

Additionally, many services communicate with social networks to indicate nearest positions or determined areas of interest. In all of these cases, electronic resistance consists of working, every day, to prevent abuse of such systems and to seek increased legal process and oversight during the phases of data collection and location surveillance.

Monitoring individuals and their behaviors is also achieved with the so-called online behavioral tracking, essentially a record of web browsing activities. New web technologies have generated untold possibilities for companies and authorities, allowing them to observe the behavior patterns of web users and the additional possibilities of monitoring Internet navigation and personal interest, from super cookies or automatic advertisement related to electronic mail content to secret codes included in printers, which allow the identification of not only the printer but also, potentially, of the individual using it, and can even produce invisible codified information.

Also threatening, and by now found nearly everywhere: in libraries and schools, in government offices and private companies, are RFID systems.

Thus EFF's FOIA transparency project is particularly interesting in this sense as well, given that in addition to its other activities it also aims to oblige a number of agencies to reveal their policies regarding control, investigation, data collection and

even surveillance of individuals on social networks performed without legal process or oversight.

Another fascinating example of constructive electronic activism is the *HTTPS Everywhere* project, which is still in beta-version, is an extension of the *Firefox* browser created in collaboration with the TOR project and EFF allowing the encryption of communications a number of major websites. This system effectively resolves issues with https encryption over multiple sites, rewriting all requests to sites offering encryption support to https. This significantly reduces vulnerability to active attacks and traffic analysis, and facilitates the activation of enhanced security features (for those sites that offer them). Obviously, it is not possible to make use of this software on those sites, or portions of sites, which do not support https.

Still within the realm of Internet privacy, but having different aims, is EFF's *TOSBack* project, where TOS stands for *Terms of Service*, and which keeps a check on the changes to terms of service and user policies of the many highly frequented sites for the purposes of monitoring change over time to clauses and liability limitations and correlating them to user rights, including the confidentiality and security of any customer data provided to those sites.

3.4.5 EPIC Activities in the Field of Privacy

It is not possible to discuss the protection of privacy in the digital era without mentioning EPIC (the *Electronic Privacy Information Center*), an association which, for years, has worked on issues of enormous importance and interest.

Body scanners, for example, are one of the most important objectives of their activism: EPIC seeks to suspend the installation of these instruments and to carry out an emergency independent review of their functionality, settings, and ability to memorize information, and frequently makes the increasing actual security.

Cloud computing is another hot topic to which EPIC frequently dedicates it activities: this is a technology that raises considerable privacy and security risk issues, in addition to doubts regarding data retention, given that users, once they have consigned their documents, photos, and videos to "the cloud", no longer have direct control over that data. The greatest risk of cloud computing, however, is that materials and personal data stored in this way could conceivably be accessed by unauthorized third-parties. EPIC also cites web-based medical services as being not only extremely delicate but also at risk, and therefore worthy of significant control by activists; not only delicate but also hugely present in the lives of many is *Facebook*, which EPIC frequently takes to task for a number of issues regarding personal privacy and Internet security. Biometric data collection is yet another topic generating significant discussion: consider that during the course of the United States military presence in Iraq a biometric database containing approximately 750,000 records was created; if this data were to fall into the wrong hands, it would certainly create an extremely dangerous situation, especially in regions susceptible to religious and ethnic unrest.

It became apparent in 2007, in fact, that the American troops were using mobile fingerprint and retina scanners on Afghan and Iraqi citizens at checkpoints, in workplaces and on the battlefield, creating an enormous database of these citizens managed by the American military.

3.4.6 Transparency

The final field of operations of electronic activists is, as previously mentioned, that of transparency.

New technologies have the potential to facilitate increasingly democratic relationships between the public sector and the citizens it serves. Today a set of new instruments provide individuals with increased possibilities of not only monitoring governments and private enterprises, but also the real possibility to accompany any accusations of cover-ups, censorship, or corruption with concrete documentation.[8] Promoting and utilizing all these tools which facilitate increased transparency is clearly beneficial, just as controlling the growth of the so-called "state technologies" is also undoubtedly beneficial. Similar attention, however, should also be paid to our own Internet Service Providers: for example, verifying whether our providers voluntarily interfere with *BitTorrent* connections, block *VoIP* calls, or otherwise counteract the principals of net neutrality. Testing our own internet connections, and collecting proof of any ISP activities of this sort can also contribute to increased transparency. A software program developed by EFF, Switzerland, was created with exactly this aim: it is an open source program for testing the integrity of data communications over networks, ISPs and firewalls, advising users when IP packets are forged or modified, and when anti peer-to-peer, censorship, packet control or advertising systems are employed.

Finally, mention must be made in this section of electoral verification systems, especially with regard to rights connected to electronic voting and the best modalities of verifying the correct implementation of such delicate procedures.[9]

[8] The New York Civil Liberties Union released, in 2012, a free smartphone application for witnessing an unlawful police stop and recording the moment. The app "allows people to record videos of and report police 'stop and frisk' activity, a practice widely denounced by civil rights groups as unjustified stops that they say mostly target minorities and almost never results in an arrest" (Leitsinger 2012). Donna Lieberman, NYCLU Executive Director, stated that "Stop and Frisk Watch is about empowering individuals and community groups to confront abusive, discriminatory policing […]The NYPD's own data shows that the overwhelming majority of people subjected to stop-and-frisk are black or Latino, and innocent of any wrongdoing. At a time when the Bloomberg administration vigorously defends the status quo, our app will allow people to go beyond the data to document how each unjustified stop further corrodes trust between communities and law enforcement"(Lieberman 2012).

[9] See Sect. 3.10.

3.5 A New Perspective on Hacking

3.5.1 The Essence of Hacking

Games. Ideas. Rebellion. Skill. Creativity. Curiosity. The desire, and the need, to think outside the box. The essence of hacking is especially this last element, which is, more than anything else, a phenomenon that despite popular belief and despite its frequent association with the world of crime, can justly lay claim to truly noble origins and has as its principal and most treasured elements the uninterrupted flow of creativity and ideas, even those that are unconventional and at times even unfeasible, its opposition to authority and its nearly always playful approach.

Originating in world-class universities such as MIT, Stanford, UC Berkeley, and Harvard, it was nurtured by academics who were not afraid to reach deep, many of whom then went on to write some of most important pages of the history of the computer to date, going far beyond the rules and grids commonly followed by the market and scientific communities and outside habitually adopted schemes. Hacking has breathed life into inventions which have revolutionized not only programming but human communication itself, without ever losing sight of the delight in accepting challenges, and, above all, of the playfulness and of the love of the game itself, that are so typical to this world.

This aspect of playfulness has characterized this phenomenon since its origins: since those early hackers, fascinated with first gaming, and then creating experimental new programs that came to be called videogames, and since the times of those first cyber-jokes organized in university and college computer labs. Carrying out small and large undertakings, without ever taking themselves too seriously, demonstrating an unusual sense of humor, with particular enthusiasm for the cheerful side of nearly everything, games, videogames, and puzzles, are all constants that have continued, undimmed, within hacker communities, through to the current days.

However, the world of computing (and of law) has become, over the last 15 years, terribly serious. This is evidenced by the creation of a body of legislation and laws, especially criminal law, which is excessively repressive and vaunts sanctions and legal limits that are far too high, and an overprotection of infrastructure and data, clearly indicating a fear, in the vast majority of cases misdirected, regarding the possibility of terrorist attacks or criminal behavior. Then there is the deep-seated aversion to any behavior that reveals technical capacities beyond those considered "normal", as if such advanced skill might somehow jeopardize the "computer system". A less fearful (and less angry) approach to information technology, and more playful tactics to the resolution of the problems inherent to a highly computerized society might contribute to the creation of a more peaceful political and legal scenario; today, however, this is not at all the case.

An analysis of today's new forms of hacking, especially those which are politically motivated, reveals that the original aspects of play, of games, and sense of humor are decidedly less present than in the 1960s and 1970s.

The political circumstances motivating many instances of technological rebellion and of hacker activism are frequently critical, violent and repressive, and are often environments in which such actions may carry harsh penalties and in which the very lives of anyone opposing power structures is at risk.

A second interesting aspect, correlated to hacking's playful approach, is that many of the technologies currently utilized by hackers around the world were not created with a professional or political use at all, but rather for hobby, and have unexpectedly found success in other sectors.

3.5.2 The Hacker Spirit and Some Lessons from the Ushahidi Project

Each year the *Technology Review*, MIT's famous journal, honors young innovators who are changing the world of technology. The winner, in 2010, of the Humanitarian of Year award was David Kobia, a 35 year-old Kenyan who had left his country to study computer science at the University of Alabama, and who is one of the creators and developers of the already discussed open source project *Ushahidi* (which in Swahili means "testimony"). His project collects eyewitness reports, messages, blog entries and citizen journalism pieces and places them on an interactive map not only to denounce (providing as, it does, an often visual account) electoral fraud or deception, or episodes of ethnic violence, but also to make such deeds known to the entire world. Furthermore, information made available by the system also allows first responders to natural disaster or fire areas to react to the emergency more efficiently and with faster response times.

The software is as ingenious as it is easy to use. Based on the idea of the *eyewitness*, it provides visual testimonies to events occurring in those areas of the world stricken by critical social or political conditions.

These reports are presented on a map, and have been enormously helpful at times when traditional sources of information either are not accessible or supply news that is willfully distorted, incomplete or misleading. Ushahidi has already been used in a plethora of diverse regions around the world, including during the Sudan elections, to document violence in the Gaza strip, to monitor the British Petroleum oil spill in the Gulf of Mexico, during the summer fire season in Russia, and to facilitate search, rescue and aid efforts following the 2010 earthquakes in Haiti and Chile.

The software was created in 2007 as a response to uprisings in Kenya, following presidential elections there. The president, Mwai Kibabi, had declared a media black out for the entire country; Internet became the only open communication channel. At that time, David Kobia was an expat student living thousands of miles away in Birmingham, Alabama; stymied at how to help his countrymen from so far away, he came up with a map-based system to track newsworthy events, effectively using the Internet to circumvent the country's media blackout. The first version launched on the web was quite simple: it featured a map and a form to fill out indicating the

incident being reported, the time and date, the nearest city and a brief comment or description. Over the following months, the software was perfected with the addition of a more precise timeline, the ability to use the application on mobile devices and in diverse languages, the use of different maps and ability to follow determined places and events in space and time.

The project is based on an open-source platform. Given that the network of "witnesses" increases, adds maps, news events, and facts in a myriad of diverse contexts, with each new installation, the system evolves further. All reports are thoroughly checked, compared against other sources, validated and entered onto the map, utilizing different colors, usually in no more than just a few minutes.

Despite the tragic nature of the events documented (episodes of ethnic cleansing, electoral and political corruption, media blackouts, natural and man-made catastrophes and disasters), Kobia's experience demonstrates a wonderfully correct approach to rebellion and to hacking.

Thinking outside the box, seeking to provide services that have yet to come into existence, by making new use of widely available technology that *does* exist (in this particular case, cellular phones), having positive aims, such as the opposition to injustice, to authority, to fraud.

The project was initially kept simple, little more than just a game (the KISS rule so beloved by hackers worldwide: Keep It Simple, Stupid) but was based, from the very outset, on a system architecture that would allow for future global growth, involving an already existing "world" of individuals desiring (and needing) to report, to communicate, and only then thinking of how to combine forces with others having similar objectives.

Therefore, using the previous case-study as a point of departure, if we were looking for some preliminary suggestions on how to carry out digital activism with a similarly positive approach, we could consider the following points:

1. *the concept of testimony, or witnessing*. Today, throughout the world, *electronic eyes* are watching us; not only those of the states in which we live (through their strategically placed surveillance and security cameras), but also those of our fellow citizens: millions of digital cameras, smartphones, handheld video cams, webcams. The *Ushahidi* project could develop, above all, owing to the willingness of countless individuals, first in Africa, and then throughout the world, to provide a visual report of the events unfolding in their territories. It's the old rule of the reporter, who, if he is going to properly cover his news stories, needs to wear out the soles of his shoes getting to the places where facts happen. Ushahidi allows just this, on a virtual platform. This initiative was based, above all, on the need for local eyewitnesses, and on the hope that there would be a widespread interest, in these regions, in speaking out and in being heard;
2. *verifying sources*. Given the sensitive nature of this type of service, it was fundamental that it include a rapid and reliable method of verifying information before it was placed on the map and made available to the public. It is only natural: the fear of causing undue alarm, or, even worse, of spreading misinformation, is, in such cases, extremely high. And so a "cross-referencing" system was created

with other information sources, both internal (originating from the same system, for example, multiple reports on the same incident from the same place) and external (from news agencies and traditional media). This keen attention to the accuracy of information provided and to the verification of sources is by now quite rare in an electronic world in which the primary focus has become to publish news first, even if it is incorrect, partial, or even false, without pausing for objective verification. If the previous point depended on the system being nourished by an ever growing "army" of local foot-soldiers, this second aspect is related to the quality of the service offered. Finding a delicate meeting balance between the need for rapidity and the urgency of the information to be divulged, on the one hand, and a reasonable certainty that the news is also true, on the other, is certainly not an easy task. Efforts to respect this equilibrium, in fact, can sometimes counteract some of the more innovative aspects of the project, given that there is a tendency to "mediate" in order to reduce the possibility of error to a minimum. In other words, the project actively avoids becoming "too innovative" because it might then become too difficult to control in a particularly delicate environment in which no errors can be made;

3. *open system, open source*. Here, too, the *Ushahidi* project had no alternatives. The need was for the system to "create itself" over time, spontaneously originating networks as it developed, and the only way to achieve this was for the engine to drive the entire system to have the capacity to auto-replicate and to be modified or adapted to contingent situations. The open source engine allows, in this case, for part of the success and efficiency of the system to be left in the hands of those who use and perfect it;
4. *the use of even "obsolete" reporting tools*. Another winning element of the *Ushahidi* project is that of using technologies which, although in some countries may have become nearly obsolete, in many developing countries, including those for which the project was first used and developed by its coordinators, are still the most frequently available. Mobile phones, for example, are widely diffused even in countries with limited access to computers and Internet networks (Castells et al. 2007), and a simple web interface system, without graphics or animation, allows quick loading and interaction on slow connections and first generation browsers.[10] In order for the project to be successful, it would be fundamental to focus on those technologies actually available to its prospective users, a type of developer foresight that only rarely occurs.

[10] Miard, in an interesting essay (Miard 2009), remarked the importance of mobile phones as a tool for civil resistance and social protest activities in two historical events in Serbia and in Belarus: actions for bringing down Milosevic in Serbia in 2000 and, 8 years later, mobile used by Belarusian activists. In Serbia in 2000, highlights the author, mobile phones and the use of coded short-text messaging to coordinate actions, immediate street action and mobilization were a crucial tactical and operational tool, also because the Internet was slow and not used a lot in Serbia in 2000. In Belarus in 2008 all mobile phone operators were under control, but dissident groups used mobile phones to contact potential new activists and also for operative coordination, for reporting police or crowd movements, to mobilize protesters. The use of mobile phones in Belarus was limited for safety reasons (tapping from the regime and risks of localization).

5. *the full use of all currently existing alert and reporting tools*. The power of communications and networking systems such as *Twitter* and *Facebook* is by now quite well-known. Fundamental to the project was a keen desire for the system to be based on the most widely available technology platforms. The only way to do this was to make it compatible, but also able to dialog, with any communication tool that might be utilized by individuals in disadvantaged nations and areas experiencing social or political upheaval. This provided an invaluable, exponentially growing "fire power", and today the *Ushahidi* project has developed into a richly informative visual experience, transposed onto a map, which transcends barriers created by borders, distance, and diverse languages and cultures, to benefit humanity, particularly the most needy and the most disadvantaged.

3.5.3 A New Breed of Hackers

Today's hackers have accepted an inheritance, connected to the very word, which is both rich and complex in its connotations.

This new generation is quite distant from both the typical hacker figures of the second half of the last century, and from the stereotypes portrayed in film and television.

We have at times taken the liberty of classifying hackers more on the basis of what they do, for how they are changing the world, than on their actual abilities or skills: this is an approach that would have been unthinkable even a few years ago, when being a hacker was synonymous, above all, with being a computer genius, an individual with extraordinary programming talent.

However, the fact is that, in many cases, it was hackers themselves who were the first to acknowledge that "being a hacker" was, from the beginning, a concept applicable to every aspect of life and to all their actions, and not limited to technology: a way of thinking and behaving that was the full expression of the desire to bypass rules, to uncover truths, to refuse to stop at first results or to be discouraged by the first difficulties encountered.

The writer Steven Levy, in the preface of his book *Hackers*, which he dedicated to "*those computer programmers and designers who regard computing as the most important thing in the world*", sought, in layman's terms and through a careful historical analysis, to explain not only the origins, but also the importance, of this fantastic technological adventure to the general public.

Hackers was the first work on this subject to achieve a wide readership, and illustrated, especially to readers outside the computer industry, the remarkable endeavors of these new electronic rebels.

The book developed a huge following even among hackers themselves, generally distrustful of mainstream work on such subjects.

Levy began by contesting the generally accepted use of the term *hacker*, which was then used to deride those individuals, often labeled, in some circles, as

computer nerds. These individuals, in such environments, would be relegated to the edges of society – and its conventions – and emarginated, not unlike Rousseau's *promeneur solitaire* in his (unwanted) tyranny of intimacy, or adolescents with grave behavior problems in their relationships with peers, family, schools, and authority. In other cases, so went the urban myth surrounding hackers, there are programming geniuses plagued with unhappy outcomes despite considerable talent, forced to operate forever at amateur, non-professional levels, cut off from the shining world of real programmers, of software multinationals and from the profits available there.

In fact, in the world of these modern digital rebels, success now most often comes, rather than from the solitary efforts of a lone individual shut away working in his room, but as the result of strong, well-coordinated team work. Collaborative work, today, facilitates a "meeting of the minds". In other words, the idea of the hacker as a lonely nerd is rapidly disappearing. Activism requires motivation, exceptional communication skills, extraordinary programming vision, and the ability to react quickly to rapidly unfolding political, market and technological changes. There are, of course, a number of inspiring exceptions, but even opposition to censorship and to authority in general, although it may originate from the ideas of a single individual, after a certain period of time, if it is to become truly efficient, generally requires an increasingly organized and complex structure.

One of the most interesting characteristics of these new hackers/nerds is their capacity to tunnel old skills toward very new directions, nearly always in the name of freedom. The hackers (and computer nerds) of the 1960s, 1970s, 1980s and 1990s had a powerful competitive advantage in terms of access to information, as compared to those outside the world of computing. Thus, unlike the general population, they were often privy to exclusive information, which they then elaborated and put to use with their unique reasoning abilities.

Today, by contrast, there has been a sort of "leveling off" with regard to the access to knowledge: everything is generally available to anyone who cares to look for it.

It must be noted, however, that hackers, typically, have always had communication channels that are "off the beaten path", which, in typically hacker fashion, thoroughly verify all information before it is divulged and circulated.

The difference, in the behavior of the hackers described in these pages, lies in how their minds manage to re-elaborate more or less well-known information and to adapt it with a view to opposition, rebellion, the protection of freedoms and liberty: applying it, then, to concrete situations that they absolutely intend to change. However, today's hackers no longer have exclusive access to knowledge. Today the majority of technical information and specialized documentation is available to anyone with nothing more than a smartphone; there are, however, individuals who have a capacity of vision (and of foresight) that is greater than that of others, or who have witnessed facts and situations, some terrifying, that they seek to address through the use of technology. Technology which becomes an offshoot of the human mind and heart, and is then directed toward new horizons, for the good of humanity.

The present state of events merits two further considerations.

The first is that the current environment created by the Internet, which we all utilize today, in terms of accessibility to technological knowledge, was enormously influenced by the world of American university and research centers, whose *modus operandi* has always been to render public, available to all in orderly archives and academic journals, the results of their research. The availability online of the concepts at the base of hugely complex projects and their correlated standards and studies have similarly gone a long way to facilitate the development of one of the most remarkable aspects of the web: its transparency. At the same time, however, against the splendid openness of the web is aligned the world, just as important to our daily lives, of telephone service providers, electric systems, television services, which, on the contrary, have always been closed, controlled by monopolies and lobbies, and constantly plagued by compatibility and efficiency problems.

A second observation (for some: complaint) is that this enormous wealth of technical documentation has caused a sort of stratification of knowledge. Everything is available, it is true, but the complexity, even during simple operations, has increased exponentially, creating not a few practical problems.

It was said earlier in this Chapter that hacking has a noble history. It is, however, also a history which has followed an often changeable course. Over the last 60 years it has taken on diverse facets, depending on the existing technology and the varying approaches taken by academicians and users. It reached its apex, somewhat paradoxically, when these machines were not yet widely available, and, above all, were still particularly difficult to use, when the computer was still an elitarian instrument which only a few geniuses were able to assemble and to understand, when the yearning to connect to others' systems and to enter into (or break into) them was based on the dream of using resources much greater than those otherwise available, and of being able to program in new languages.

Most important, however, was the dream of learning *more*. The huge computers housed in the gyms of neighborhood schools and university computer labs, with their complex operating systems and with much better networking capabilities than those few early home models, became much sought after targets, primary objectives that allowed access to new worlds containing knowledge and contacts, and that were, above all, the entryway to the new electronic frontier. Ask a hacker of any age, from the "old schoolers" to modern day teenagers, to describe the most thrilling moment of his or her career, the instant they remember most clearly, and you will nearly always get the same answer: that first day, when, thanks to a modem, a connection, and a phone line, from the inside of their homes or school rooms, they "leaped" onto the web, leaving the confines of the physical world and entering into the "deep blue", as it is so effectively defined by the writer Jeffery Deaver in his "hacker trilogy". That very first moment when they were for the first time, in a word, *connected*.

In the present day, however, it is no longer necessary to break into university research centers for close encounters with technology. We are continually surrounded by it. At least in technologically advanced countries, the scarcity or the quality of resources

is almost never an issue.[11] Nearly everybody has, in their homes, technological means of enormous power, far more powerful than those which, in the 1960s and 1970s, were so large that they could only be found in university and school computer labs. In fact, these modern devices offer performance capabilities that are far superior than the real needs of the average user. The ordinary smartphone, costing only a few hundreds of dollars, has capacities that far outperform those of the computers found only in research facilities just a few decades ago. There is no need to hunt down technology in order to learn from it: today technology is simply inescapable, and has become intricately bound with nearly every facet of our lives. By contrast, the behavior in those years was very similar to that of the members of MIT's *Tech Model Railroad Club* in the 1950s. At night they travelled the famed tunnels of the campus grounds, picking locks to sneak into the rooms housing the first vast computers, costing millions of dollars. There was, in other words, the perceived need to physically access technology, which in those times was jealously guarded, used by an elect few.

The fact that, today, extremely powerful technology is truly available and within physical reach of us all presents, in our opinion, both negative and positive aspects. One of the negative aspects is that such complex instruments are often fairly difficult to use effectively, and require specific "user education" so that they do not create more difficulties than advantages for their users. A positive aspect is that anyone who desires to rebel, to make their voice heard, who intends to take advantage of technology for the common good, for opposition, for activism, can now do so with no other investment than his or her own culture, skill, and imagination.

3.6 The *Do-It-Yourself* Approach

This passion for computers and for machines, for gears, this veritable passion for DIY (*Do It Yourself*) is another constant in the history of hacking. The "build it yourself" approach has, from a hacker's point of view, two distinct advantages.

[11] See the interesting notion of *virtual resources* remarked by Peckham (Peckham 1998). The author outlines that: "While resource mobilization theory normally addresses tangible economic or physical resources (e.g., money, recruits), examining movement/counter-movement interaction on the Internet requires an expansion of the definition of "resources". The term "virtual resources" as I define it refers to resources that have no intrinsic value and little meaning outside the context of on-line activity, yet are highly valued by Internet users. These are resources whose worth is not measurable in terms of monetary value, but nonetheless have real consequences. Recognizing the existence of virtual resources is important in part because the internal economy of the Internet blurs common notions of production, capital, and goods values […]. In the on-line environment, the ability of a movement to take action does not necessarily require money or elite voices, but rather, as we shall see, it requires a mobilization of resources that primarily have value only to Internet users" (Peckham 1998: 322).

The first is that it presents a great challenge to skills and abilities: hackers are rarely content with simply buy a "ready to use" computer "off the shelf", but often prefer to invest time in hacking it themselves, in creating it, so that it has exactly all the specifications and options they desire.

The second advantage is based on that element of distrust in authority, and in all that is placed on the market "ready to use", which, as we will see, is often a typical characteristic of hackers.

In the world of digital activism, however, DIY may also take on yet another facet: in areas where access to even basic technology, to the Internet, and even to electricity may be a challenge in and of itself, DIY offers a way to overcome obstacles which otherwise might be insurmountable.

In Cuba and Africa there are true artists, experts in the re-assembly and use of computers which in other countries would have long ago been donated to museums. In these areas, the need to improvise with hardware, modems, and cables has led the reemergence of a real passion for the machine itself. In fact, this brings to mind the fact that when those early networks, that were to become the embryo of the Internet, which were being created, one of the key considerations was that of using easy to find materials so that in the case of disaster or catastrophe, communication would not be interrupted and it would in any case, if the need were to arise, be possible to utilize spare parts from other commonly available appliances.

Today's activist hackers, or *hacktivists*, to use a portmanteau of fairly recent creation, especially if they operate in areas that are disadvantaged or backward, in terms of technology, must have an excellent knowledge of hardware and of the situation *in loco*. In some of the most rigorous hacker milieus, the choice of hardware and of the DIY approach is motivated by interesting ideological or political positions: the desire to oppose multinationals, to refute all that is mass-market, to avoid consumer "traps" the desire to be different, to avoid any possible tracking instruments inserted in the machine. At the base of it all, there is the impulse to achieve a technical and intellectual "independence" from the industrialized world made up of identical series of mass market commercial products. Therefore, in actuality, an interpretation of the DIY approach as a refusal to submit to a rubber-stamp mentality and an expression of the individuality of hackers is not so far off at all.

It was Steven Levy again, in the second Chapter of *Hackers*, who sought to describe this "benevolent" ethic which gradually evolved in the environments where those first computers appeared and of which, it seems, not only the general public, but also politicians and governments, must be reminded, year after year.

This novel ethic was a new way of working, a dream, a rare devotion, a symbiosis between man and machine which not only had never before been seen, but had never before even been possible.

They were laying the foundations, in fact, of a veritable hacker culture, and at the same time the expertise and proficiency of the individuals involved were reaching heights never before imagined.

It was, in fact, in this context that the modern idea of *skill* was elaborated, skill as compared to a general society that is slower, that at times surrounds and suffocates these gifted minds.

3.7 The Hacker Ethic

The principles on which these individuals based their behavior were never formalized or discussed, but were silently spread, almost as though it was behavior in some way dictated by the very use of computers. The *hacker ethic* slowly came into being.

The first principal of the ethic, central and foremost, is that access to computers (and to any system that could help mankind better understand the workings of the world and society) must be free, unlimited and total. *Information must be free*. A direct consequence of this principle of freedom is the idea of "*the hands-on imperative*" the right, the duty to have access to, to touch, to possess not only computers themselves but also the knowledge they contain and convey.

According to Levy, the idea that an essential lesson on how computers worked could be had only by "opening one up and taking it apart", observing how it worked and using this knowledge to create something new, even more interesting than the first was far from new, but was to become a pillar of the hacker ethic.

A similar attitude among today's hackers causes them to resent any person, physical barrier or law that tries to keep them from gaining access to or changing something which, to their minds, require changing.

Levy cites the well known fact that one of the most irritating situations for a hacker is the existence of systems they consider to be imperfect.

The idea that *all information should be free* is a second central tenet of the hacker ethic and is fundamental to hackers' way of thought. If there is no access to information, with a view to improving existing technology, the entire system will collapse. The free exchange of information serves to augment the collective creativity and saves energy, eliminating the need to "reinvent the wheel" time and time again.

Together with these two closely-connected concepts – that computers should be accessible to all and that information must be free – there is also a clear and deep-seated distrust of authority in all its guises, and a marked preference for decentralization.

Hackers were convinced that the best way to achieve a world based on the free circulation of information was to guarantee an open system, without confines and without boundaries separating them and that information that they so needed to advance their paths toward knowledge.

Bureaucracy was perceived, even by those first hackers, as a hostile and damaging phenomenon, to be overcome and done away with, whether it be at a university, local or national government, or a multinational corporation.[12]

All of these factors – bureaucracy, the centralization of power in the hands of government, dehumanization – are nothing more than defective and dangerous systems, given that they are incapable of facilitating the natural instinct to explore. Most bureaucracies, for example, are based on arbitrary rules, unlike, as Levy writes, the elegance of computer logic and algorithms.

Alongside these cardinal principles of the hacker ethic, there are several secondary but equally interesting aspects.

The original hackers, for example, maintained that an individual should be judged solely on the basis of his or her skill, and not on the basis of age, social class, race, sex or even education. This concept of meritocracy essentially took two forms: what you knew about computers, and what the community to which you belonged thought you knew about computers. Discussing meritocracy in modern society (and politics), where the concept is by now not only obsolete but often derided, has a certain nostalgic ring to it, but, by contrast, it remains one of the fundamentals of the modern hacker world, on which few are willing to compromise in any way. Your worth is based on who you are, your reputation on what you do in your community, even if you are still only a teenager, even if you are, according to popular standards, a "loser". This meritocratic approach would be an excellent example to follow for many sectors today. However, this, unfortunately, is not the case.

Hackers' activities, writes Levy, were far different from the clichés that surrounded them and that aimed to downplay the importance of their actions.

These individuals, above all, were markedly different from the humiliating stereotype, so widely accepted in our culture, of the bespectacled, badly dressed, calculator-in-shirt pocket computer nerd. Fortunately, over the course of recent years, this definition has undergone something of a change and now focuses more on the extraordinary intelligence of these individuals rather than on any social problems, real or imagined.

Levy, in fact, seeks to emphasize that, notwithstanding any relationship difficulties that they may or may not have had, hackers were, above all, extraordinary adventurers,

[12] See the interesting essay by Juris regarding new digital media and activist networking within anti-corporate globalization movements (Juris 2005). The author outlines how anti-corporate globalization activists have used new digital technologies to coordinate actions, build networks, practice media activism, and physically manifest their emerging political ideals and notes: " […] activists have used e-mail lists, Web pages, and open editing software to organize actions, share information, collectively produce documents, and coordinate at a distance, reflecting a general growth in digital collaboration. Indymedia has provided an online forum for autonomously posting audio, video, and text files, while activists have also created temporary media hubs to generate alternative information, experiment with new technologies, and exchange ideas and resources. Influenced by anarchism and the logic of peer-to-peer networking, more radical anti-corporate globalization activists have thus not only incorporated new digital technologies as concrete networking tools, they have also used them to express alternative political imaginaries based on an emerging network ideal" (Juris 2005: 192).

visionaries, who faced real risks, putting themselves always on the line. They were artists in the full sense of the word, and the only ones who truly comprehended the reasons why the computer would become such a revolutionary instrument, the only ones who incessantly exchanged ideas and who understood, day after day, how far things could be pushed: the *hacker mode*. Thus, far from being a derogatory appellation to be ashamed of, indicating a plethora of personal problems, being a hacker had become a respected badge of honor, to be worn with pride.

When Levy, in preparation for his book, met with hackers of all ages, from those who operated in the 1950s and wanted to "get their hands on" those first enormous computers secreted away in large institutions to the underground hackers of the 1980s, he realized that there was a very solid common link that connected them all, their ethic, a code of behavior that was widely shared and diffused, a philosophy, which seemed to progress in close symbiosis, noted Levy, with the same of elegance of the code and the programs appearing on the screens of those "young wizards" of a new age, who so skillfully used them. It was, writes the author, a sort of philosophy based on sharing, on openness, on decentralization, on the urge to get, at any cost, *hands on* those machines in order to improve them, and, consequently, to improve the world.

This sort of "primordial ethic", concluded Levy, was the gift of those first hackers to their own generation, one which they hoped would be handed down to future generations as well.

A heredity which, in fact, would become equally important for all those who had never even had any interest at all for computer science or for computers, o who (erroneously) thought that they would never be touched by technological advances. Those hackers not only were the first to clearly see the magic of computing before all the rest of us, but they freed it for humanity and they worked and they fought so that all of us, several decades later, are now able to reap the maximum benefit. In order to achieve this, it was necessary to understand the workings of the machines and their functioning at the highest possible capacities.

These principles, so general and abstract, have in many circles survived untouched to our times as well.

If we observe, even superficially, the actions of today's hackers, it is immediately apparent that aspects such as opposition to authority, the sharing new information, openness and decentralization are still surviving, and in some cases, have a far greater potential for expression, given that today's generations have at their disposal technology that does much to facilitate these objectives.

3.8 Hacking and Crime

One aspect seems quite clear: among the hacker principles described by Levy, that which is today most widely diffused is, without a doubt, a keen awareness of the fundamental importance of *working together*, something that modern technology, as any teen or twenty-something will be able to explain at length, has rendered quite

easy to do (just as it is now much easier to mobilize forms of protest and large numbers of people in just a few hours, or minutes).

Even the dynamic concept of hacking itself, or, better stated, the *actions* that concretely constitute hacking, have changed over time, mutating, modernizing, and updating their perspectives.

The original spirit of hacking was based on a quest for transparency, on the ardent desire to guarantee the unlimited circulation of information, on the public intention to render and to maintain computing, and technological resources in general, available to all.

This was accompanied by a dose of mistrust of authority and of the public sector in general, and even more, by an unconcealed hostility toward multinationals, telephone companies, toward whoever dared to develop closed, obscure source code, toward state-technologies riddled with hidden backdoors, access points that permit authority to enter and control user systems at any time, or toward systems and microprocessors defined as "trusted" by their producers but that are in fact potential control instruments themselves. The engine behind it all was curiosity, supported by (and made possible) by extraordinary technical skills, and a keen desire to hack the system.

The 1990s, and the wide-scale diffusion of Internet and the home personal computer that this period ushered in, sent the entire panorama into something of a crisis. The distinction between hacker and computer criminal became, in the common perception, blurred and confused. The two terms were intentionally superimposed and used synonymously by diverse news agencies and by scholars and pseudo-scholars of the phenomenon.

Labeling hackers as criminals is, without a doubt, more interesting than discussing them from the point of view of the battle to safeguard our liberties, of the defense of rights, of their role as rebels in an increasingly controlled society, as enemies for the *Big Brother*. Highlighting the dark side of hacking is more lucrative for the media, more advantageous for authority and for the political world, more intriguing, at times, for certain self-proclaimed hackers who try in vain to reconcile the hacker ethic with certain types of behavior which are clearly, and quite simply, criminal.

The often-referred to "dark side" of hacking, although certainly evocative, is frequently little more than mere illicit behavior on the part of criminals more interested in illegal profit than in satisfying any sort of intellectual curiosity. And such conduit has *nothing* to do with the generous and unselfish origins of hacking, as described previously in this chapter.

Unfortunately, it is undisputed that the last 20 years have been, in this sense, fairly deleterious. Even attempts to distinguish between hackers and crackers or between hackers and cyber-criminals have dwindled (although attempts are still at times made, during conference debates and round tables and in articles and comments posted throughout the web), and at this point, in common parlance, the expression hacker has taken on a menacing connotation, (erroneously) denoting nighttime attacks on military and civilian systems, data destruction, sabotage of critical infrastructure, wide-scale fraud and even terrorist activities.

It is evident that the line between crime (understood as the violation of a law) and non violent, exemplary protest actions, in the name of determined ethical principles, can very well constitute a difficult minefield to traverse. It must be remembered, however, that many of the behaviors of the digital dissidents that we will describe have indeed violated one if not several laws, often criminal, that have been adopted by the countries in which they live, and therefore such actions are, in the strict sense, crimes. Here I have in mind rebellion against copyright principles, committed for the sake of the diffusion of knowledge, in overt violation of IP law, or of the diffusion of reserved documents, which may violate state security laws, or again of actively working to break down and circumvent state censorship and firewall systems. Thus much of this "criminal behavior" has no criminal intent whatsoever, but seeks only to oppose a system deemed to be unjust.

It is important to appreciate the profoundly diverse psychological approach, the completely different "criminal mind", of those who violate a financial system in order to then offer security consultation for a tidy profit or those who use proxies and anonymous web browsers to commit crime or to recycle illicit funds from, in rather sharp contrast, those who operate on shady limits of legality in the name of principles held by many to be sacrosanct and emblematic of freedom itself. In our opinion, it is fairly easy to recognize hackers from the real criminals: it is sufficient to consider the motivations, the rationale behind the behavior. The spirit of hacking shines through, then, without a great many doubts as to its interpretation.

Toward the end of the 1980s the term hacker became fused (and confused) with the meaning "computer criminal". This resulted in three particularly unpleasant consequences: a distortion, in the perception of the general public, of the sense of the actions of so many individuals, and the beginning of large scale investigations and court cases, a great many of which were revealed to be little more than modern day witch hunts, signaling one of the darkest moments in the history of hacking. The motivations for this distortion are, to my mind, diverse. First of all, the intentionally excessive and alarmist attention paid by the international press to the exploits of a few hackers in the United States. A second consequence was the issue of statements and announcements by law enforcement agencies proclaiming the need for vigorous investigative and legal actions aimed at striking back at that then new and (it was claimed) terribly serious form of crime. Finally, a legal fabric which formed slowly, with the first laws specifically aiming at punishing cybercriminals, and which was almost immediately revealed to be confused, ineffective, and, in some cases, perfect for branding as criminal those borderline activities that do in fact belong to the world of hacking but which pose no threat whatsoever to society.

Today, seen from a distance of so many years, the majority of those frenetic activities against real or perceived computer crimes of the 1980s and 1990s appear clearly to have been attempts to curb from the outset a phenomenon that disquieted the powers of state, and not, as officially maintained at the time, a necessary reaction to real economic damages, attacks against critical infrastructures or widely diffused social alarm.

In that period, the same tactic was maintained with regard to the war against the unauthorized duplication of software (quickly defined with the already loaded and denigratory term of *piracy*[13]). Violators were threatened with disproportionately heavy penal sanctions, with the aim of protecting interests that were essentially economic, rather than social or in any way related to public security. For example, in Italy, the investigation of the first cases of "suspected computer crime" reported by the press involved nothing more than the "much feared" phenomenon of unauthorized duplication of computer programs. In fact, however, the real source of concern in those days was the ever growing presence of computers themselves. Hackers instilled fear, in national and local authorities, due less to what they actually did and more on the basis of their very existence and numbers; they instilled fear due to what they might *potentially* do. For the first time in history, it was actually feasible that an ordinary citizen, without any special military or espionage training, might conceivably, from the comfort and safety of his own home, be in the position to attack or even paralyze the central nervous system of a sovereign state. Therefore, hackers, the only ones to have the skills necessary to plausibly enact such an attack, were immediately placed on "extremely dangerous persons" lists in countries throughout the world, to be punished with repressive *ad hoc* laws and legislation. It is of course easy to understand how the criminal aspect of hacking, or even the possibility of a criminal aspect of hacking, has often sparked sometimes vitriolic debate, even within the hacker community itself.

At this point we would like, before continuing further, to draw a set of clear distinctions: the mere fact that a computer expert is arrested does not automatically mean that he or she is a criminal, nor indeed a computer criminal. A person can certainly be arrested, for example, because he has acted in the pursuit of ethical and commendable aims under a regime that sanctions such behavior, or, to the contrary, because he has, in fact, "simply" behaved like a criminal. And different again is the case of a computer criminal who has been tried and convicted, for example, of espionage (and of receiving payment for those illegal activities) or of having penetrated computer systems for the purposes of extortion, from that of a hacker arrested

[13] See the interesting study by Dahlberg regarding the terms *pirate* an *piracy* and their evolution in the legal and political world (Dahlberg 2011). The author notes: "Since pirates, as a rule, operate on the open sea, it may seem natural that this liquid form of digital information attracts information pirates of various kinds: cyber criminals, file sharers, hackers, hacktivists, and ordinary media users. Whereas the cyber criminal may be seen as an individual moving from one kind of criminal habitat to another, the term "file sharer" refers to the use of file-sharing technology, regardless of whether the "sharing" is legal or illegal. The aspect of criminal intent (mens rea) is also ambiguous when defining a hacker, who typically finds a way to enter a computer system less to steal information than to prove his (hackers are usually male) computer skills. The hacktivist, by contrast, uses his or her sophisticated knowledge of computer systems to acquire and distribute sensitive economic and political information. Because of the changing nature of contemporary media products and media content, which increasingly consist of digital devices and digital information, the ordinary media user may not only be using pirated copies (knowingly or not), but may also be acting like a pirate (without necessarily being aware of it)" (Dahlberg 2011: 265).

for having broken into his country's state security system in order to simply make public his thoughts, or for having breached security systems not for personal profit but with the aim of guaranteeing the free circulation of information or the protection of consumers, or for having made public classified information that is of use for to the entire community. Based on these distinctions, it seems to me that it is, in fact, not so difficult to construct an initial qualification, by objectively analyzing the *motivations* giving rise to such actions.

Another typical, but at times somewhat confusing, distinction often applied in and to the hacker community is that of white hat and black hat hackers. Sometimes included in the black hat category are expert hackers who have, for shorter or longer periods of their lives, systematically violated the law: breaking into government computer systems, copying software, data, codes, passwords, credit cards and causing system damage. The white hat hackers, on the other hand, are those who chose to work within the confines of the law, or who break laws only accidentally, while pursuing other aims, for the common good or simply to satisfy their own curiosity.

In reality, of course, the two categories are almost never really comparable at all, and in recent years, even the connotation of the black hat hacker as an ex-criminal is little more than a nuance. In the white hat category are generally found noted hackers such as Steve Wozniak, Linus Torvalds, Tim Berners-Lee and Richard Stallman, individuals who have written the history of computer science, creating hardware and software still in use today.

The black hat category, on the other hand, features individuals who are often just as well known, but more for their singular capacities and talent for breaking laws: experts in breaching security systems of all kinds, who, once they have paid their dues to society, made fruitful use of their skills to enter the world of business, or who have courted organized crime or frequented other criminal environments.

To my mind, it is complicated to group these two such diverse categories in a single *genus*, even with different colored hats. I have however noted that the term black hat continues to be used frequently, and that it continues to carry a particularly meaning-laden punch, especially in the collective imagination of laymen everywhere. Evidently the "dark side of the force" continues to focus attention on this issue, and to fascinate us all.

3.9 Threats to Hackers

3.9.1 The EFF Report Unintended Consequences

In a report entitled "*Unintended Consequences. Twelve Years under the DMCA*" published in February 2010[14] to mark the 12-year anniversary of the passing of the

[14] See https://www.eff.org/files/eff-unintended-consequences-12-years.pdf. Accessed 21 November 2011.

Digital Millennium Copyright Act (DMCA) in the United States, Fred Von Lohmann, of EFF, listed a series of cases involving hackers who had had the misfortune to run up against the provisions of the DMCA, which prohibit not only the *circumvention* of copyright protection measures, but also prohibit the *distribution of tools* and *technologies* used for circumvention.

These measures clearly create the risk of rendering illegal all those actions of hackers who seek to "crack" a particular system, even out of mere curiosity.

The ease with which it is possible to put the provisions of this act to use in order to send out cease-and-desist notices or to commence legal proceedings has as a clear consequence, as stated previously, not only the increased likelihood of a complete block of scientific research activities but also the unjust stifling of the freedom of speech. As is noted in opening remarks:

> In practice, the anti-circumvention provisions have been used to stifle a wide array of legitimate activities, rather than to stop copyright infringement. As a result, the DMCA has developed into a serious threat to several important public policy priorities: The DMCA Chills Free Expression and Scientific Research. Experience with section 1201 demonstrates that it is being used to stifle free speech and scientific research. The lawsuit against 2600 magazine, threats against Princeton Professor Edward Felten's team of researchers, and prosecution of Russian programmer Dmitry Sklyarov have chilled the legitimate activities of journalists, publishers, scientists, students, programmers, and members of the public. The DMCA Jeopardizes Fair Use. By banning all acts of circumvention, and all technologies and tools that can be used for circumvention, the DMCA grants to copyright owners the power to unilaterally eliminate the public's fair use rights. Already, the movie industry's use of encryption on DVDs has curtailed consumers' ability to make legitimate, personal-use copies of movies they have purchased. The DMCA Impedes Competition and Innovation. Rather than focusing on pirates, some have wielded the DMCA to hinder legitimate competitors. For example, the DMCA has been used to block aftermarket competition in laser printer toner cartridges, garage door openers, and computer maintenance services. Similarly, Apple has used the DMCA to tie its iPhone and iPod devices to Apple's own software and services. The DMCA Interferes with Computer Intrusion Laws. Further, the DMCA has been misused as a general-purpose prohibition on computer network access, a task for which it was not designed and to which it is ill-suited. For example, a disgruntled employer used the DMCA against a former contractor for simply connecting to the company's computer system through a virtual private network ("VPN") (EFF report 2010).

The preamble is clear: despite the legislation had been expected to protect copyright, has demonstrated the capability of influencing other sensitive sectors of society. First of all, scientific freedom, and freedom of expression, when used as a lever to achieve indirectly a second result, to silence the scientific community. But also a restriction of competition, of fair use, of the chance to explore and share.

3.9.2 Some Significant Recent Legal Cases: Cease-and-Desist Actions

The EFF Report includes references to a number of interesting recent legal cases.

In 2009, Apple Computers threatened legal action against the free hosting site *BluWiki*, accusing site directors of hosting a discussion, among a number of hobbyists,

on the topic of reverse engineering of iPods in order to permit use of non-Apple and non-iTunes software and applications. Without this type of intervention, owners of iPods and iPhones have been be unable to use third-party software to sync their media collections from computers to their Apple devices. The material on the public wiki was merely a discussion of the reverse engineering effort, and there were no "circumvention tools" made available nor any indication that the hobbyists had succeeded in their efforts. Nevertheless, Apple's lawyers sent *OdioWorks*, the company behind BluWiki, a cease-and-desist letter threatening legal action under the DMCA. The text of the letter is the following:

> It has come to our attention that a website you operate, www.bluwiki.com, is disseminating information designed to circumvent Apple's FairPlay digital rights management system. […] FairPlay is considered anti-circumvention technology under the Digital Millennium Copyright Act. The DMCA explicitly prohibits the dissemination of information that can be used to circumvent such technology […] Apple therefore requests that you immediately disable the thread at http://bluwiki.com/go/Ipodhash. Please notify me by reply e-mail once you have done so, and feel free to contact me if you have any questions.[15]

BluWiki, in turn, sued Apple, maintaining that the discussions in question fell under the sphere of free speech and were thus protected by the *First Amendment*. In response, Apple dropped its threats.[16] EFF's defense strategy included five points:

1. the wiki pages in question included only "information," which is to say discussions conducted via text. There was nothing on those pages that could constitute a "technology, product, service, device, component, or part thereof," falling within the scope of the DMCA's anti-circumvention provisions;

---

[15] See the full takedown notice at https://www.eff.org/files/filenode/odio_v_apple/Exhibit%20A.pdf. Accessed 23 October 2011.

[16] See the announcement by EFF on 22 July 2009: "Apple has retracted its legal threats against public wiki hosting site Bluwiki, and, in response, EFF is dismissing its lawsuit against Apple over those threats. The skirmish involved a set of anonymously authored wiki pages in which hobbyists were discussing how to enable recent-vintage iPods and iPhones to 'sync' media with software other than Apple's own iTunes (e.g., Songbird or Winamp). We're not talking about any 'piracy' here; we're talking about syncing the media you legitimately own on the iPod or iPhone you own, using software of your choice. In November 2008, Apple sent a series of legal threats to the operator of Bluwiki, alleging that these hobbyist discussions about interoperability violated the DMCA's anti-circumvention provisions, even though the author(s) of the pages hadn't yet figured out how to accomplish their goal. So, according to Apple, even talking about reverse engineering for interoperability violates the DMCA! In a later letter, Apple also alleged that short excerpts of decompiled code on the pages infringed its copyrights, despite the fact that the code fragments related to a trivial function and comprised a tiny fraction of the iTunes software overall. […] While we are glad that Apple retracted its baseless legal threats, we are disappointed that it only came after 7 months of censorship and a lawsuit. Moreover, Apple continues to use technical measures to lock iPod Touch and iPhone owners into using Apple's iTunes software. And just last week, Apple used an update to iTunes as an excuse to lock the new Palm Pre smart phone out of using Apple's iTunes software. In light of these developments, you can be sure that perfectly legal efforts to reverse engineer Apple products will continue in order to foster interoperability. We hope Apple has learned its lesson here, and will give those online discussions a wide berth in the future". https://www.eff.org/deeplinks/2009/07/apple-backs-down-blu. Accessed 23 October 2011.

2. the information was intended to afford iPod owners access to the iTunesDB files on their own devices;
3. the technical measure being discussed on the Bluwiki pages does not appear to be one that "effectively controls access" to the iTunesDB files within the meaning of 17 U.S.C. § 1201(a)(3)(B);
4. the information contained on the Bluwiki pages appears to be "for the purpose of enabling interoperability of an independently created computer program with other programs," and therefore protected by the reverse engineering exemption to the DMCA's anti-circumvention provisions;
5. judicial precedents interpreting and applying the DMCA's anti-circumvention provisions have made it clear that circumvention does not fall within the reach of the statute unless it has some nexus with copyright infringement.[17]

A related case, which received wide coverage by the international press, involved the vulnerability of the rootkits in thousands of Sony-BMG music CDs. Professor J. Alex Halderman, at the time a student at the University of Princeton, discovered the existence of several security vulnerabilities in the CD copy-protection software of a number of Sony-BMG titles. He delayed publishing his discovery for several weeks while consulting with lawyers in order to better understand the applicability of the DMCA to that particular type of set of circumstances (Halderman and Felten 2006). Nonetheless, the security flaws[18] were subsequently publicized by another researcher who was apparently unaware of the legal risks created by the DMCA (or was simply less cautious). In October 2003 Halderman was threatened with legal action, based on the same provisions of the DMCA, after having published a report (Halderman 2003) documenting vulnerabilities in copy-protection software produced by *SunComm*. Halderman revealed that merely holding down the shift key on a Windows PC would render SunnComm's copy protection technology completely ineffective:

> […] in tests on a newly-released album, I find that the protections may have no effect on a large fraction of deployed PCs, and that most users who would be affected can bypass the system entirely by holding the shift key every time they insert the CD (Halderman 2003).

The company threatened legal action but withdrew the threats when the matter was rendered public, preferring to avoid the negative press attention. This episode highlights the fact that security researchers may be threatened with legal action for simply seeking to publish pertinent and even essential consumer information.[19]

---

[17] See the response at the address https://www.eff.org/files/filenode/odio_v_apple/Exhibit%20E.pdf. Accessed 23 October 2011.

[18] The authors note: "The systems are surprisingly complex and suffer from a diverse array of flaws that weaken their content protection and expose users to serious security and privacy risks. Their complexity, and their failure, makes them an interesting case study of digital rights management that carries valuable lessons for content companies, DRM vendors, policymakers, end users, and the security community" (Halderman and Felten 2006: 1).

[19] See also the concluding statements in the essay by Wu, Craver, Felten and Liu (Wu et al. 2002) describing the attacks on SDMI audio watermarks: " […] (1) weaknesses in the watermarking design are very likely to be explored by an adversary as effective attacks, prompting the need of thorough testing by watermark designers; (2) a large amount of information regarding the embedding.

In September 2000, the *Secure Digital Music Initiative* (SDMI) issued a public challenge encouraging skilled technologists to try to defeat certain watermarking technologies intended to protect digital music. Professor Ed Felten of Princeton University and his team of researchers accepted the challenge and succeeded: they managed to remove the watermarks. When Professor Felten and his team tried to present their results at an academic conference, however, SDMI representatives threatened the researchers with liability under the DMCA provisions. Moreover, threatening letters were also delivered to the researchers' employers and to conference organizers. The conclusions of the paper were as follows:

> We have defeated all four of their audio watermarking technologies, and have studied and analyzed their "non-watermarking" technologies to the best of our abilities given the lack of information available to us and given a broken oracle in one case. Some debate remains as to whether our attacks damaged the audio beyond standards measured by "golden ear" human listeners. Given a sufficient body of SDMI-protected content using the watermark schemes presented here, we are confident we could refine our attacks to introduce distortion no worse than the watermarks themselves introduce to the audio. Likewise, debate remains on whether we have truly defeated technologies D and E. Given a functioning implementation of these technologies, we are confident we can defeat them (Craver et al. 2001: 11).

Pamela Samuelson discussed these anticircumvention rules as a threat to science (Samuelson 2001), stating that:

> Scientists who study encryption or computer security or otherwise reverse engineer technical measures, who make tools enabling them to do this work, and who report the results of their research face new risks of legal liability because of recently adopted rules prohibiting the circumvention of technical measures and manufacture or distribution of circumvention tools. Because all data in digital form can be technically protected, the impact of these rules goes far beyond encryption and computer security research. The scientific community must recognize the harms these rules pose and provide guidance about how to improve the anti-circumvention rules (Samuelson 2001).

Hewlett-Packard, too, resorted to the DMCA to threaten researchers who had made public a security flaw in HP's Tru64 UNIX operating system. The group of researchers, known as *Secure Network Operations* ("SNOsoft"), had released software in 2002 that demonstrated vulnerabilities in the system. In this case as well, legal action was withdrawn once it came to attention of the press. It is interesting to note, however, that, in 2003, *Secure Network Operation* had already made its policy concerning full disclosure quite clear:

> I have been following the subject of full disclosure for a while, and as most of you know, have dealt with some of the issues that full disclosure can cause (HP/Secure Network Operations/DMCA). While the idea of full disclosure is a good idea, and while we support

---

mechanism derived from pairs of original and watermarked signals, can be used to build powerful attacks, prompting the need of obscuring distinct traces between original and watermarked signals. The second point, though not having received much attention in the literature, is important for SDMI applications. Due to various limitations of the challenge including the very short time frame, we adopted practical strategies to increase our chance in finding successful attack(s) and in understanding all four watermark challenges. We focused on finding attacks that render misdetection by a watermark detector without significantly degrading perceptual quality. These are crucial start points from which many optimizations, improvement, and fine-tuning can be made" (Wu et al. 2002: 4).

> it, we feel that the exploit source code should not be released to everyone. It is possible to prove a vulnerability exists by releasing well written advisories. Because of this fact, proof of concept code (exploit source) is not a requirement for the education of the possibly vulnerable. Releasing non-malicious exploit code is also not an option as any local script bunny/kiddie can easily render it functional. Proof of concept code is useful for legitimate contract based penetration tests. It is also useful for study as it demonstrates fundamental flaws computers today (not built in security). But again, proof of concept code is not for everyone. […] With that said, Secure Network Operations, Inc. will no longer be releasing functional proof of concept code. We may release sufficiently detailed advisories.[20]

In April 2003, the educational software company *Blackboard Inc.* used a DMCA threat to stop the presentation of research on security vulnerabilities in its products at the *InterzOne* conference in Atlanta. The security flaws that researchers sought to reveal to the public involved the ID cards used by university campus computer systems. The presentation was blocked as the result of a cease-and-desist letter:

> "Please be advised that the actions described on Mr. Hoffman's website, including the hacking of Blackboard's system, are illegal, and that any effort by either Mr. Hoffman or Mr. Griffith to convey to others at your Conference any information gleaned in whole or in part from such actions, particularly in an effort to cause Blackboard economic harm, would be improper. Please be advised of our view that it would be actionable for you or your conference to facilitate Mr. Hoffman's and Mr. Griffith's announced plans for, among other things, the disclosure of signals captured, the releasing of code, the description of development of functional readers, and the hardware specs to wire the readers and/or control circuits. […] Accordingly, Blackboard hereby requests that you immediately cease and desist from any disclosure of information noted above, or any facilitation of that disclosure, including but not limited to, the disclosure of signals captured, the releasing of code, the development of functional readers, and hardware specs to wire the readers and control circuits")[21] which was delivered shortly before the beginning of the conference ("Dear Interz0ne II Conference Chair: […] I am attaching a cease and desist letter relating to the "Campuswide System Vulnerabilities Update" seminar, listed on your schedule for Saturday, April 12, at 7:00 pm, with panelists Billy Hoffman ("Acidus") and Virgil Griffith ("Virgil"). I urge you to read the attached letter before that seminar begins, so that you may take any and all appropriate actions").[22]

In 2003, U.S. publisher John Wiley & Sons abandoned plans to publish a book by researcher Andrew "Bunnie" Huang, citing DMCA liability concerns. Wiley had commissioned Huang to write a book that described certain security flaws in the Microsoft Xbox game console which that Huang had discovered as part of his doctoral research at M.I.T. (Huang 2002) Only after a number of years had passed was the young man finally able to self-publish his book.

Another hacker to be openly threatened was Seth Finkelstein, a researcher specializing in "particular" projects: his work focused on "censorware" software (i.e., programs that block web sites that contain objectionable material), and he was able to document security flaws and other failings in a number of systems of this

[20] See http://seclists.org/fulldisclosure/2003/Jan/306. Accessed 21 November 2011.

[21] See http://www.interz0ne.com/events/interz0ne_cease_order.html. Accessed 21 November 2011.

[22] See http://www.interz0ne.com/events/interz0ne_cease_order.html. Accessed 21 November 2011.

type. Finkelstein's research, for example, revealed that censorware vendor N2H2 in fact blocked a variety of completely legitimate web sites. This information was transformed into valuable legal evidence when the researcher was asked to assist the ACLU in the course of legal proceedings commenced in Massachusetts to challenge a law requiring the use of web filtering software by federally-funded public libraries. N2H2 was able to claim that the provisions of the DMCA should effectively block researchers like Finkelstein from examining its software.

Another well-known hacker, who lives each day on the razor's edge, is Benjamin Edelman: he has conducted extensive research regarding flaws in various censorware products. Edelman's research has also produced important legal evidence: the most famous case was a court challenge[23] brought by activists against the Children's Internet Protection Act (CIPA), which sought to mandate the use of censorware by public libraries.

In July 2001 another DMCA case attracted worldwide attention: a young Russian programmer, Dmitry Sklyarov, who had been invited to speak at the famous DEFCON hacker conference in Las Vegas, was jailed for several weeks in the United States.[24] Prosecutors, prompted by software goliath Adobe Systems Inc., alleged that Sklyarov had worked on a software program known as the Advanced e-Book Processor, which was distributed over the Internet by his Russian employer,

[23] See the ACLU FAQ page on this case at http://www.aclu.org/technology-and-liberty/benjamin-edelmans-lawsuit-faq. Accessed 26 October 2011. "A computer researcher named Benjamin Edelman, represented by the ACLU, has filed this suit to establish his First Amendment and "fair use" right to examine the full list of sites contained in an Internet blocking program and to share his research tools and results with others. […] Blocking programs such as N2H2's are notoriously inaccurate, often preventing access to sites that should not be blocked while failing to block many that should. And blocking programs are increasingly used in public schools and libraries and by various government agencies. Because of this growing public role, it is especially important that the public be able to check and evaluate how these programs work, and what Web sites are being blocked. However, most blocking program companies, like N2H2, consider their block lists to be proprietary trade secrets, and will only distribute them in an encrypted form that the program itself can understand but people can't. As a result, current and potential customers, including schools and libraries, cannot effectively evaluate the program's accuracy, and students, library patrons and other citizens forced to use blocking software are kept in the dark about the extent of Web site censorship. […] Ben Edelman […] would like to continue his research on N2H2, but cannot proceed further without being able to access and examine its full list of blocked sites. To do this he will have to 'reverse engineer' N2H2's program to figure out what security measures are preventing him from reviewing the list. With that information he can create a software tool to 'circumvent' those measures and create a readable version of the list for review. He then wants to publish the block list, the circumvention tool that he used to get the list, and the results of his analysis of the list. Given the increasing role of blocking programs as an official means of censoring use of the Internet, the kind of research Ben does is an important means for citizens to monitor the software and its potential for abuse".

[24] Criminal Complaint, United States v. Dmitri Sklyarov, Case No. 4 01 257 (N.D. Cal. July 7, 2001), available at http://www.eff.org/IP/DMCA/US_v_Elcomsoft/20010707_complaint.html. Accessed 21 November 2011.

ElcomSoft.[25] The software allowed owners of Adobe electronic books ("e-books") to convert them from Adobe's e-Book format into PDF files, thereby removing restrictions embedded into the files by e-book publishers. In December 2002, a jury acquitted Elcomsoft of all charges. See, *inter alia*, the study of Yen on this issue (Yen 2003), explaining the correlation between federal gun control laws and DMCA anti-trafficking provisions. According to the author:

> A casual observer of Sklyarov's plight might wonder how a man who writes a computer program for translating documents from one format to another can face up to a $500,000 fine and 5 years in jail while a corporation that makes lethal rifles suffers no consequences when one of its weapons is used to kill 10 people. Interestingly, the explanation lies - at least partially - in the federal government's stern reaction to the use of digital technology, especially the Internet, to commit copyright infringement (Yen 2003: 3).

As is increasingly evident, researchers in the fields of security vulnerability, hacking and cryptography deal on a daily basis with matters which tend to place them at significantly higher risk for both civil and criminal legal actions. Such scenario not only frustrates legitimate research efforts, thus conceivably inhibiting discoveries that might otherwise benefit the entire society, but may also even result in court proceedings for the researchers.

The comment of the world-renowned security expert Bruce Schneier regarding the Sklyarov case is clear (Schneier 2001):

> On 16 July in Las Vegas, the FBI arrested a Russian computer security researcher, because he presented a paper on the strengths and weaknesses of software used to protect electronic books. Because of the Digital Millennium Copyright Act (DMCA), which makes publishing critical research on this technology more serious than publishing nuclear weapon design information, Dmitry Sklyarov (age 27) landed in jail. Just how did the United States of America end up with a law protecting the entertainment industry at the expense of freedom of speech? […] I attended Dmitry Sklyarov's talk at DefCon. What he did was legitimate security research. He determined the security of several popular E-Book reader products and then notified the respective firms of his findings. His company Elcomsoft published, in Russia, software that circumvented these ineffectual security systems. His DefCon talk was a clear and evenhanded presentation of the facts. He said, in effect: 'This security is weak, and here's why'. (One particular company he mentioned stored the password in plaintext inside the executable. So, anyone with Notepad and a few minutes of scrolling could have the book modified for easy distribution.) The FBI nabbed him at the request of Adobe Systems, Inc. for breaking the security on Acrobat's E-Reader API, and held him without bail. Welcome to 21st Century America, where the profits of the major record labels, movie houses, and publishing companies are more important than First Amendment rights. In many ways, we're seeing the legacy of the NSA's long war against cryptography and cryptographic information. Until the late 1990s, the NSA used the threat of

[25] As Yen correctly notes in an articulated essay regarding federal gun control norms and the DMCA's anti-trafficking provisions (Yen 2003): "In July of 2001, Russian computer programmer Dmitry Sklyarov traveled to the United States to speak at a conference in Las Vegas, Nevada. While in Las Vegas, Sklyarov was arrested and charged with violating the Digital Millennium Copyright Act ('DMCA'). According to the complaint against him, Sklyarov's offense was the writing and distribution of software that enabled translation of documents written in the Adobe Corporation's Secure eBook Format to the more common Portable Document Format (PDF). To the surprise of many, Sklyarov found himself facing a fine of up to $500,000 and up to 5 years in prison. The federal government held Sklyarov in custody for 3 weeks before a court released him on $50,000 bail. Sklyarov eventually managed to avoid the charges against him by agreeing to testify against his employer Elcomsoft" (Yen 2003: 2).

> national security to prevent the dissemination of encryption technologies. When they could, they blocked the publication and dissemination of information. When that failed, they concentrated on products, using both legal and illegal methods to block encryption software. Many people believe the NSA's primary rubric, export controls, would not stand up to a constitutional challenge, but it was never tested. The NSA eventually gave up. […] The entertainment industry is behaving in the same way. The DMCA is unconstitutional, but they don't care. Until it's ruled unconstitutional, they've won. The charges against Sklyarov won't stick, but the chilling effect it will have on other researchers will. The entertainment industry is fighting a holding action, and fear, uncertainty, and doubt are their weapons. We need to win this, and we need to win it quickly. Please support those who are fighting these cases in the courts: the EFF and others. Every day we don't win is a loss. (Schneier 2001).

Another famous case is that of the Dutch cryptographer (and security systems analyst) Niels Ferguson, who discovered a major security flaw in Intel's HDCP video encryption system (Crosby et al. 2001). Ferguson openly declared that he had decided against publishing his results on his website on the grounds that he travels frequently to the United States and is fearful of "prosecution and/or liability under the United States DMCA law" (Ku 2005). His considerations are the following (Ferguson 2001):

> I have written a paper detailing security weaknesses in the HDCP content protection system. I have decided to censor myself and not publish this paper for fear of prosecution and/or liability under the US DMCA law. […] I travel to the US regularly, both for professional and for personal reasons. I simply cannot afford to be sued or prosecuted in the US. I would go bankrupt just paying for my lawyers. I want to make it quite clear that Intel, who developed the HDCP system, has not threatened me in any way. But the threat does not come only from Intel. The US Department of Justice could prosecute me. Any other affected party, such as a movie studio whose films are protected with HDCP, could sue me under the DMCA. That is a risk I cannot afford to take. The simple alternative would be to never travel to the US again. This would harm me significantly, both professionally and personally. It would lock me out of many conferences in my field, and keep me away from family and friends. It all sounds a bit too far-fetched, right? Who would sue over the publication of an article? Well, there are very good reasons to believe that I risk a lawsuit if I publish my paper. A team of researchers led by Professor Edward Felten was recently threatened with a DMCA-based lawsuit if they published their own scientific article. The resulting court case is still pending. (Ferguson 2001).

In other cases, important conferences[26] on hacking or on computer security issues have been organized, or moved beyond the confines of certain nations in order to avoid this type of intimidation or to avoid the applicability of United States law.

[26] See, incidentally, an interesting Cory Doctorow's debate about the arrests of bloggers and activists after net freedom conferences (Doctorow 2012). He quotes (and remarks) the words of James Losey, from the New America Foundation: "I noticed a pattern of people getting arrested, detained, or sentenced following Internet Freedom conferences. The timing is coincidental, but its a poignant reminder of the risks people face when pushing back against unjust authority and fighting for basic rights […] In late October 2011, Alaa Abd El Fattah, a prominent Egyptian blogger, was arrested as he returned from the Silicon Valley Human Rights Conference. The charge: inciting violence toward the military during riots on Oct. 9, 2011. He was released nearly 2 months later. That same month, Jacob Appelbaum, a core member of the Tor Project who has also volunteered with Wikileaks, was detained in Iceland after speaking at the Internet and Democratic Change, an event sponsored by the Swedish government. And just last month, Thai blogger Chiranuch Premchaiporn, aka Jiew, went from a speaking engagement at Google's Internet at Liberty conference in Washington to a sentencing hearing. She faced up to 20 years in prison because comments posted on her website by readers were deemed insulting to the king. In the end, she was fined the equivalent of $630 and received an eight-month suspended sentence". (Doctorow 2012).

The magazine *2600* became the object of legal action openly seeking to aiming to censure information and the freedom of the press when it published DeCSS (Eschenfelder et al. 2005), a software program that is able to circumvent DVD copyright protection; one of the most noteworthy aspects of this particular case is that the threat of civil action against 2600 was prompted by some of the most important film studios in the United States.

In yet another episode, in 2009, Texas Instruments threatened three bloggers with legal action after they had posted comments regarding the reverse engineering of the TI-83 Plus graphing calculator, a device containing technical measures that prevent users from installing alternative operating systems. When a hobbyist reverse engineered this system in order to help others run their own "home brew" operating systems, he wrote about it online. Those results generated a great deal of online commentary, including that of the three bloggers in question. TI promptly sent the bloggers letters threatening legal action under the DMCA, despite the fact that the aim of the bloggers' initiatives was in no way connected to illegal duplication activities but was purely in the spirit of further research and in order to permit a legally possessed device to perform at its maximum potential.

In the spring of 2000, Microsoft invoked the DMCA against the Internet publication forum *Slashdot*, demanding that forum moderators delete a forum post containing materials relating to Microsoft's proprietary implementation of an open security standard known as *Kerberos*. The text of the letter stated:

> Dear Internet Service Provider: We understand that your website, http://www.slashdot.org, is a popular site for developers to discuss topical issues of interest. In that vein, it has come to our attention that there have been numerous posts of concern related to Microsoft's copyrighted work entitled 'Microsoft Authorization Data Specification v. 1.0 for Microsoft Windows 2000 Operating Systems' and we would appreciate your posting this email to the site to help relay our position to your users. […] This notice is being sent under the provisions, and following the guidelines, of the Digital Millennium Copyright Act of 1998 (DMCA) […] Included on http://www.slashdot.org are comments that now appear in your Archives, which include unauthorized reproductions of Microsoft's copyrighted work entitled 'Microsoft Authorization Data Specification v.1.0 for Microsoft Windows 2000 Operating Systems' (hereafter 'Specification'). In addition, some comments include links to unauthorized reproductions of the Specification, and some comments contain instructions on how to circumvent the End User License Agreement that is presented as part of the download for accessing the Specification. […] Under the provisions of the DMCA, we expect that having been duly notified of this case of blatant copyright violation, Andover will remove the above referenced comments from its servers and forward our complaint to the owner of the referenced comments. […] We request immediate action to remove the cited violations from Andover's servers, in accordance with the provisions of the Digital Millennium Copyright Act of 1998.[27]

In the *Slashdot* forum, several individuals alleged that Microsoft had changed the open, non-proprietary Kerberos specification in order to prevent non-Microsoft servers from interacting with Windows 2000. Many speculated that this move was intended to force users to purchase Microsoft server software.

[27] See the letter at http://slashdot.org/story/00/05/11/0153247/microsoft-asks-slashdot-to-remove-readers-posts

Even Luigi Auriemma, an independent Italian researcher, attracted the attention of GameSpy's lawyers after publishing details on his web site regarding security vulnerabilities in GameSpy's online services, including a voice chat program. The cease-and-desist letter[28] was sent despite the fact that Auriemma resides in Italy and is thus beyond the reach of the DMCA.

The American cryptographer Philip Zimmermann is perhaps the best-known example of a scientist, who, from the outset has been threatened and pursued due to his research activities.

In June 1991 he created and made available at no charge the program *Pretty Good Privacy* (PGP), a data encryption and decryption software that swiftly became an international standard (Zimmermann 1995), allowing users to maintain the privacy and confidentiality of their personal digital data.

Due to his having created the PGP program, Zimmermann was sued by the firm *RSA Data Security Inc.* for alleged violation of an RSA algorithm, and accused by the United States government of illegally exporting cryptographic instruments.

As Zimmermann declared with regard to this episode:

> PGP is free software. Anyone may download it on the Internet, or from many Bulletin Board Systems. It has stirred up some controversy, because it has become a worldwide de facto standard for Email encryption, despite US export restrictions. Initially published in the US, this package has spread by the diffusion that is common to free software packages, with its 'forbidden' flavor giving it an extra popularity kick. Oddly enough, the US Government may have inadvertently contributed to PGP's spread, by making it more popular because of my case. I am under criminal investigation because of PGP's spread overseas, which the Government holds is in violation of US export restrictions. My case has captured a lot of press attention, in part because journalists realize that if an American can be imprisoned for electronically publishing something in the USA, then journalists may themselves be at risk in tomorrow's world of electronic newspapers on the information highway. Another reason why the press is so interested in my case is the Government's attempts to suppress public access to strong cryptography. The Clinton administration is trying to get the phone companies to put a special encryption device into every telephone. They expect it to take many years to accomplish this. When this 'Clipper chip', as it's called, is manufactured by the Government, they place a unique encryption key in each chip, and keep a copy of the keys in a vast government database, for wiretap purposes. Your telephone will someday have Big Brother inside. The Government hopes that the American public will accept this government-controlled cryptography, and is trying to discourage other forms of cryptography that they do not control. One way that they discourage it is by the use of export restrictions on cryptographic software. This draws PGP into the press spotlight. The US State Department has a list of items that may not be exported without a license. The Munitions List. Mostly weapons, but included in that is encryption software. Encryption software may not be exported without a license, and that license is hard to come by if the software uses advanced encryption techniques that the Government can't easily break. Software like PGP. The State Department allows items on the munitions list to be exported if they grant a Commodities Jurisdiction (CJ) for it, allowing it to be handled under the

[28] See the letter at the address http://aluigi.altervista.org/misc/75395-1.pdf. Accessed 25 October 2011.

> jurisdiction of the Commerce Department instead of the State Department. A CJ allows the item to be legally exported from the US. It would be politically difficult for the Government to prohibit the export of a book that anyone may find in a public library or a bookstore. The State Department has already granted a CJ for another book containing cryptographic source code, Bruce Schneier's 'Applied Cryptography'. So, we're putting the PGP source code in a book, which may be scanned in with OCR (optical character recognition) software. And we are applying for a CJ. It will be interesting to see where this process leads (Zimmermann 1995).

Neither of these legal proceedings amounted to anything whatsoever; the accusation of illegal exportation was dropped in 1996, and the RSA controversy was not only settled out of court but was followed by a collaboration between RSA and Zimmermann for the creation of the successive versions of the software. Twelve years later, however, on 21 September 2001, the Washington Post hosted an article based on an interview with Zimmerman, which stated that Zimmerman felt guilty about the possibility that the terrorists responsible for the 9/11 Twin Tower attacks might have used PGP during the preparation of the attack (Eunjung Cha 2001). Zimmermann responded to the article, objecting that even if his technology had been used for the preparation of violence, that act would not make him change his mind with regard to the fundamental importance of cryptography for the protection of privacy and civil liberties in the information age. He went on to state he had in fact given considerable thought to the possibility of his software being used by terrorists, or criminals in general., but that, in his opinion, that risk was outweighed by the fact that PGP had become an important tool for the protection of human rights throughout the world, as had been the original intent. Cryptography, according to Zimmermann, does far more good than harm in a free and democratic society.

> […] I felt bad about the possibility of terrorists using PGP, but that I also felt that this was outweighed by the fact that PGP was a tool for human rights around the world, which was my original intent in developing it ten years ago. […] In these emotional times, we in the crypto community find ourselves having to defend our technology from well-intentioned but misguided efforts by politicians to impose new regulations on the use of strong cryptography. […] Did I re-examine my principles in the wake of this tragedy? Of course I did. But the outcome of this re-examination was the same as it was during the years of public debate, that strong cryptography does more good for a democratic society than harm, even if it can be used by terrorists. Read my lips: I have no regrets about developing PGP. The question of whether strong cryptography should be restricted by the government was debated all through the 1990's. This debate had the participation of the White House, the NSA, the FBI, the courts, the Congress, the computer industry, civilian academia, and the press. This debate fully took into account the question of terrorists using strong crypto, and in fact, that was one of the core issues of the debate. Nonetheless, society's collective decision (over the FBI's objections) was that on the whole, we would be better off with strong crypto, unencumbered with government back doors. The export controls were lifted and no domestic controls were imposed. I feel this was a good decision, because we took the time and had such broad expert participation. Under the present emotional pressure, if we make a rash decision to reverse such a careful decision, it will only lead to terrible mistakes that will not only hurt our democracy, but will also increase the vulnerability of our national information infrastructure. PGP users should rest assured that I would still not acquiesce to any back doors in PGP (Zimmermann 2001).

3.10 Hacking Electronic Voting Machines for the Purpose of Transparency

The fear that a *democratic* electronic voting system based on the use of *obscure code* might reveal damaging flaws, is highly topical in a number of areas of the world and in the thoughts of many ordinary citizens who use these new systems when they go to the polls.

Consider the analysis of a typical *Electronic Voting System* published in the Kohno, Stubblefield, Rubin and Wallach study, featuring a security analysis of the system's source code (Kohno et al. 2004). The conclusions are unambiguous (emphasis mine):

> We found *significant* security flaws: voters can trivially cast multiple ballots with no built-in traceability, administrative functions can be performed by regular voters, and the threats posed by insiders such as poll workers, software developers, and janitors is even *greater*. […] we believe that an appropriate level of *programming discipline* for a project such as this was not maintained. In fact, there appears to have been *little quality control* in the process […] we believe that an *open process* would result in more careful development, as more scientists, software engineers, political activists, and others who value their democracy would be paying attention to the quality of the software that is used for their elections. […] The model where individual vendors write *proprietary code* to run our elections appears to be *unreliable*, and if we do not change the process of designing our voting systems, we will have no confidence that our election results will reflect the will of the electorate. We owe it to ourselves and to our future to have robust, well-designed election systems *to preserve the bedrock of our democracy* (Kohno et al. 2004: 21).

A similar *distrust* towards the efficiency of electronic voting systems is evident in a 2006 documentary, *Hacking Democracy*,[29] which garnered an *Emmy* for investigative journalism. This project represents a forceful critique of electronic electoral system used in the United States of America, and, in particular, of the technology produced by *Diebold Election Systems*. In *Hacking Democracy*, the protagonists are a number of citizens investigating anomalies in the e-voting system during the 2000 and 2004 elections, especially in Florida. The hackers' attention is focused on the trustworthiness of the management of the votes, and ends quite dramatically with the on-camera hacking of the e-voting system used in Florida's Leon County. The documentary illustrates several hacking techniques: voting machine records and other technical material are obtained from trash, and the data found is compared to interviews with former employees in a bid to obtain further information. Subsequently, the documentary followed a series of practical tests on five devices conducted by two hackers, Dr. Herbert Hugh Thompson and Harri Hursti. Both scholars illustrate different methods of *tampering the data*. The first effective system was achieved by editing the database file containing the total votes, a "forged" file in standard *Microsoft Access* that may be accessed and modified without having to enter a password. In all states where it had been imposed by law to disable the

[29] See http://www.hackingdemocracy.com/. Accessed 5 November 2011.

Access standard in order to increase the difficulty of altering the voter database, the hackers were able to circumvent the protection by developing an *ad hoc* code in *Visual Basic* language. These first "hacks" proved effective but presented, at the same time, an obvious limitation: all alterations made could be discovered by outside parties simply by comparing the results indicated in the database with "physical" paths from the tape of the machine. The hack, ultimately, would not have resisted that simple comparison.

The documentary featured a second hacking technique as well, and was a hack of the actual computer code on the memory card of the electronic voting machines. This new type of attack, developed by the hacker Harri Hursti and now known as the *Hursti Hack*, "fooled" the machine by *removing* legitimate votes from the winner and assigning the victory to the *wrong* candidate. Hursti has demonstrated that it is enough to have access to the memory card, and not the entire system, to wreak havoc with the e-voting systems analyzed, using operations that are completely *undetectable* to both supervisors and the device under attack: both would otherwise report irregularities without delay. This second type of attack, as expected, resulted in violent reactions from *Diebold*, which objected to the documentary's inaccuracy. Numerous scholars, on the other hand, including computer scientists from the University of California, Berkeley, have succeeded in reproducing Hursti's hack, and many have attested to the fact that the security threat posed by these machines is real.

The first point of reflection arises from the consideration that a voting system is, in a context of computer security, extremely *critical*, and, therefore, should be *transparent* or, in any case, should certainly always undergo a significant *hardening* process during its development phase (attacks during its development in order to reduce vulnerability); for the same reason, the computer code utilized should be *open* or *accessible*.

At the base of the policy of certain corporations producing similar devices is the patently incorrect belief that maintaining the *secrecy* of the code on which a system is based serves to protect the system. In point of fact, however, this is not an appropriate method to achieve that end, especially if this same technology, that by now has so many proven security issues in the United States of America, is also used in Canada, in the United Kingdom and in various European and Latin American countries. An obvious case such as this clearly illustrates a fundamental principle: each critical service, software or technology used in the public sphere (whether it is for the election systems, certified e-mail, smartcards for university exams, or other services) must be *open* and *transparent* and, above all, controlled by an independent party to certify its safety and security.

The motivations fostering for the hostility on the part of citizens and associations dedicated to this issue, in the United States but in other countries as well, is evident. First of all, over 20 American states do not require the *registration* of all printed votes (thus precluding the possibility of any *comparison* in case of suspected error of the electronic machinery), despite the fact that is has been conclusively demonstrated recently that errors may occur, and that thousands of votes may be lost in this operation (for example: the elections of 2004). It is also impossible for voters to

verify the correct functioning of e-voting systems and that votes are recorded without error and also makes election recounts all the more difficult. At the same time, the current situation allows the corporations producing and selling these machines and the technicians servicing them to operate without any control or oversight. Finally, in many cases, using software kept in secrecy, that has not been publicly verified in terms of its security and real operation, often may justly raise concerns among experts. Thus, it comes as no surprise to learn that in the United States of America, secrecy of the specific workings of electronic voting systems has also given rise to several significant instances of litigation.

In the 2005, in the Diebold v. North Carolina Board of Elections case, the corporation *Diebold Election Systems* filed suit against the *North Carolina Board of Elections* in order to avoid the application of a law that required vendors of electronic voting instruments to ensure that persons delegated by the state ("officers") could access the system's *source code* in order to verify vulnerabilities. The EFF intervened, filing a motion for the dismissal of the case. Although the North Carolina Board of Elections certified the equipment without reviewing the code, EFF renewed its legal action. Diebold then took the drastic decision to remove its e-voting systems from the territory of North Carolina. In a subsequent dispute, which again saw Diebold as a protagonist, the object of dispute was the presence, on a number of web sites, of comments documenting several security flaws. Diebold attempted to silence the discussion by sending hundreds of cease-and-desist letters to several Internet Service Providers hosting the confidential documents, forcing the removal of the same due to violation of copyright law; the ISPs defended their positions by appealing to the protection of their rights to free speech under the First Amendment to the Constitution.

Matt Zimmerman, counsel for the EFF, on March 15, 2007, was summoned to testify before the *House Subcommittee on Elections* with regard to the relationship between open source and voting systems in the United States of America.[30] The EFF attorney declared that the choice between an *open* and a *closed* code was of extreme importance and, above all, able to affect the efficiency of an entire system. An open code would bring more benefits than a closed code, and an open source software program would be able to manage such a critical service without any problems. According to Zimmerman, to make the use of open source software mandatory would not represent a panacea, but would ensure more transparency and would result in greater confidence on the part of potential voters regarding the functioning of the entire system. Zimmerman noted that:

> This discussion is about many things, but at its heart is the real issue of how the current generation of voting systems has relegated, in a structural way, real transparency to a secondary value. […] First, election monitoring, as a general matter, suffers in its ability to uncover and act upon useful information. Despite many documented problems through many election-monitoring efforts, despite these documented problems which are often not

[30] See the complete document at http://www.gpo.gov/fdsys/pkg/CHRG-110hhrg35805/pdf/CHRG-110hhrg35805.pdf. Accessed 5 November 2011.

> documented by election officials themselves, incidents were not investigated or investigated in only a limited way by the very election officials and vendors whose decisions and actions were at issue. Second, and more important from my standpoint, postelection litigation aimed at investigating such suspect machine performance and correcting problems that appear to have resulted in incorrect election outcomes have fared little better […] a common thread that holds us all together is a shared belief that whatever the individual technological solution turns out to be, secrecy cannot continue to operate as a cornerstone of electronic administration. Voters want to be able to cast ballots and to have their ballots counted, but even more than that, they need to be convinced that the process is a fair and accurate one. This perpetually increasing interest of the general public in the literal mechanics of the electoral process is, to borrow a computer programming term, a feature and not a bug. This is a good thing, not a bad thing. And I respectfully suggest that Congress should not be in the business of trying to dissuade the public from prioritizing transparency over a single component of the proprietary interest of vendors (Zimmerman 2007: 37–38).

Bruce Schneier, security expert, in outlining the *minimum requirements* that a system for electronic elections should have, clearly states that it is a question of *election security*. The scholar identifies the electronic devices as a threat to a clear referendum process: being computer-based, voluntary or accidental actions of a few could affect the entire system. The solution, in Schneier's opinion, resides in providing printed voting receipts to every voter, which may subsequently, should the need arise, be verified by the voter at any time, and even counted again if necessary. In short, the ideal would be to use these machines only as systems capable of generating a voting track. The four initial requirements to ensure that a system is safe, according to Schneier, are (i) simplicity, (ii) uniformity, (iii) verifiability, and (iv) transparency. The recording of voting should be as simple as possible, the system should be standard and uniform throughout the country, the votes should be verifiable, and copies should be available on paper, and all computer code used in voting machines should be made public and examined by an objective third party to detect any errors (Schneier 2008: 117).

The security analysis of an Indian electronic voting machine (obtained from an anonymous source) described in a recent study (Wolchok et al. 2010) is also quite enlightening. The machine is *vulnerable* to serious attacks that can *alter election results* and violate the secrecy of the ballot, and the team demonstrates two attacks, implemented using custom hardware, which could be carried out by dishonest election insiders, or other criminals, with only brief physical access to the machines. These two attacks involve physically tampering with the EVMs' hardware. The authors first demonstrate how dishonest election insiders or other criminals could alter election results by replacing parts of the machines with malicious look-alike components. Such attacks are made far simpler and cheaper by the EVMs' minimalist design, and they could be accomplished without the involvement of any field-level poll officials. Second, they show how attackers could use portable hardware devices to extract and alter the vote records stored in the machines' memory, allowing them to change election outcomes and violate ballot secrecy. This attack is technically straightforward, because the EVMs do not use even basic cryptography to protect vote data internally. It could be carried out by local election officials without being detected by the national authorities or the EVM manufacturers' agents. (Wolchok et al. 2010).

The conclusions are manifest:

> Despite elaborate safeguards, India's EVMs are vulnerable to serious attacks. Dishonest insiders or other criminals with physical access to the machines can insert malicious hardware that can steal votes for the lifetime of the machines. Attackers with physical access between voting and counting can arbitrarily change vote totals and can learn which candidate each voter selected. These problems are deep rooted. The design of India's EVMs relies entirely on the *physical security of the machines* and the *integrity of election insiders*. This seems to negate many of the security benefits of using electronic voting in the first place. The technology's promise was that attacks on the ballot box and dishonesty in the counting process would be more difficult. Yet we find that such attacks remain possible, while being potentially more difficult to detect. It is highly doubtful that these problems can be remedied by simple upgrades to the existing EVMs or election procedures. Merely making the attacks we have demonstrated more difficult will not fix the fundamental problem: India's EVMs do not provide transparency, so voters and election officials have no reason to be confident that the machines are behaving honestly (Wolchok et al. 2010: 13).

A fully independent security study of a *Diebold AccuVote-TS* voting machine (Feldman et al. 2007), including its hardware and software, shows that the machine is vulnerable to extremely serious attacks. For example, as the authors note, an attacker who obtains physical access to a machine, or its removable memory card, for as little as one minute, could install malicious code. Malicious code on a machine could *steal* votes undetectably, modifying all records, logs, and counters to be consistent with the fraudulent vote count it creates. An attacker could also create malicious code that spreads automatically and silently from machine to machine during normal election activities, a sort of voting-machine virus (Feldman et al. 2007).

The authors have constructed working demonstrations of these attacks in their laboratories. Mitigating these threats will require changes to the voting machines' hardware and software and the adoption of more rigorous election procedures. The team detailed *four principal points*:

1. malicious software running on a single voting machine can steal votes with little risk of detection. The malicious software can modify all of the records, audit logs, and counters kept by the voting machine, so that even careful forensic examination of these records will find nothing amiss. The team has constructed demonstration software that carries out this vote-stealing attack (Feldman et al. 2007);
2. anyone who has physical access to a voting machine, or to a memory card that will later be inserted into a machine, can install said malicious software using a simple method that takes as little as 1 min. In practice, poll workers and others often have unsupervised access to the machines (Feldman et al. 2007);
3. *AccuVote-TS* machines are susceptible to voting-machine computer viruses that can spread malicious software automatically and invisibly from machine to machine during normal pre and post election activity. The team has constructed a demonstration virus that spreads in this way, installing a demonstration vote-stealing program on every machine it infects. The demonstration virus spreads via the memory cards that poll workers use to transfer ballots and election results, so it propagates even if the machines are not networked (Feldman et al. 2007);

4. while some of these problems can be eliminated by improving *Diebold*'s software, others cannot be remedied without replacing the machines' hardware. Changes to election procedures would also be required to ensure security (Feldman et al. 2007).

References

Barlow, John Perry. 2000. Censorship 2000. http://www.isoc.org/oti/articles/1000/barlow.html. Accessed 14 November 2011.

Castells, Manuel, Mireia Fernández-Ardèvol, Jack Qiu Linchuan, and Araba Sey. 2007. *Mobile communication and society*. Cambridge/London: MIT Press.

Craver, Scott A., Min Wu, Bede Liu, Adam Stubblefield, Ben Swartzlander, Dan S. Wallach, Drew Dean, and Edward F. Felten. 2001. Reading between the lines: Lessons from the SDMI challenge. http://www.usenix.org/events/sec01/craver.pdf. Accessed 23 Oct 2011.

Crosby, Scott, Ian Goldberg, Robert Johnson, Dawn Song, and David Wagner. 2001. A cryptanalysis of the high-bandwidth digital content protection system. http://www.cypherpunks.ca/~iang/pubs/hdcp-drm01.pdf. Accessed 23 Oct 2011.

Dahlberg, Leif. 2011. Pirates, partisans, and politico-juridical space. *Law and Literature* 23(2): 262–281.

Doctorow, C. 2012. Internet freedom activists arrested/detained after Internet freedom conferences. http://boingboing.net/2012/06/09/internet-freedom-activists-arr.html. Accessed 10 June 2012.

EFF Report. 2010. Unintended consequences: Twelve years under the DMCA. https://www.eff.org/wp/unintended-consequences-under-dmca. Accessed 23 Oct 2011.

Eschenfelder, Kristin R., Anuj C. Desai, Ian Alderman, S.Joanna Sin, and Shen Yi. 2005. The limits of DeCSS posting: A comparison of internet posting of DVD circumvention devices in the European Union and China. *Journal of Information Science* 31(4): 317–331.

Eunjung Cha, Ariana. 2001. To attacks' toll add a programmer's grief. http://www.washingtonpost.com/ac2/wp-dyn/A1234-2001Sep20. Accessed 23 Oct 2011.

Feldman, Ariel J., J. Alex Halderman, and Edward W. Felten. 2007. Security analysis of the Diebold AccuVote-TS voting machine. https://jhalderm.com/pub/papers/ts-evt07-init.pdf. Accessed 4 Nov 2011.

Ferguson, Niels. 2001. Censorship in action: Why I don't publish my HDCP results. http://catless.ncl.ac.uk/Risks/21.61.html

Godwin, Mike. 1998. Cyber rights: Defending free speech in the digital world.

Halderman, Alex J. 2003. Analysis of the MediaMax CD3 copy-prevention system. https://jhalderm.com/pub/cd3/. Accessed 23 Oct 2011.

Halderman, Alex J., and Felten, Edward W. 2006. Lessons from the Sony CD DRM episode. https://jhalderm.com/pub/papers/rootkit-sec06.pdf. Accessed 23 Oct 2011.

Huang, Andrew "bunnie". 2002. Keeping secrets in hardware: The Microsoft XBoxTM case study. http://web.mit.edu/bunnie/www/proj/anatak/AIM-2002-008.pdf. Accessed 23 Oct 2011.

Juris, Jeffrey S. 2005. The new digital media and activist networking within anti-corporate globalization movements. *The Annals of the American Academy of Political and Social Science* 597: 189–208.

Kohno, Tadayoshi, Adam Stubblefield, Aviel D. Rubin, and Dan S. Wallach. 2004. Analysis of an electronic voting system. http://avirubin.com/vote.pdf. Accessed 7 Nov 2011.

Ku, Vicky. 2005. A critique of the digital millenium Copyright Act's exemption on encryption research: Is the exemption too narrow? http://www.yjolt.org/files/ku-7-YJOLT-465.pdf. Accessed 16 Oct 2011.

Leitsinger, M. 2012. App records, reports controversial police 'stop and frisk' practice. http://usnews.msnbc.msn.com/_news/2012/06/08/12124572-app-records-reports-controversial-police-stop-and-frisk-practice. Accessed 11 June 2012.

Lessig, Lawrence. 2009. *Remix: Making art and commerce thrive in the hybrid economy*. New York: Penguin Press.

Lieberman, D. 2012. NYCLU releases "Stop and Frisk Watch" phone app to fight back against NYPD stops. http://www.nyclu.org/news/nyclu-releases-stop-and-frisk-watch-phone-app-fight-back-against-nypd-stops. Accessed 11 June 2012.

McLure, Helen. 2000. The wild, wild web: The mythic American West and the electronic frontier. *The Western Historical Quarterly* 31(4): 457–476.

Miard, Fabien. 2009. Mobile phones as a tool for civil resistance. Case studies from Serbia and Belarus. http://www.digiactive.org/wp-content/uploads/research3_miard.pdf. Accessed 22 Oct 2011.

Peckham, Michael. 1998. New dimensions of social movement/countermovement interaction: The case of scientology and its internet critics. *The Canadian Journal of Sociology* 23(4): 317–347.

Samuelson, Pamela. 2001. Anticircumvention rules: Threat to science. *Science* 293(5537): 2028–2031.

Schneier, Bruce. 2001. A security technologist's view. Bruce Schneier discusses the Sklyarov case and the DMCA. http://www.cfdr.eu.org/files/schneier_flyer.pdf. Accessed 23 Oct 2011.

Schneier, Bruce. 2008. *Schneier on security*. Indianapolis: Wiley.

Tolbert, Caroline J., and Ramona S. McNeal. 2003. Unraveling the effects of the internet on political participation? *Political Research Quarterly* 56(2): 175–185.

Wolchok, Scott, Eric Wustrow, J. Alex Halderman, Hari K. Prasad, Arun Kankipati, Sai Krishna Sakhamuri, Vasavya Yagati, and Rop Gonggrijp. 2010. Security analysis of India's electronic voting machines. https://jhalderm.com/pub/papers/evm-ccs10.pdf. Accessed 4 Nov 2010.

Wu, Min, Scott A. Craver, Edward W. Felten, and Bede Liu. 2002. Analysis of attacks on SDMI audio watermarks. http://www.ece.umd.edu/~minwu/public_paper/icassp01_sdmi.pdf. Accessed 23 Oct 2011.

Yen, Alfred C. 2003. What federal gun control can teach us about the DMCA's anti-trafficking provisions. http://www.chicagoip.com/yenarticle.pdf. Accessed 23 Oct 2011.

Zavestoski, Stephen, Stuart Shulman, and David Schlosberg. 2006. Democracy and the environment on the internet: Electronic citizen participation in regulatory rulemaking. *Science, Technology, & Human Values* 31(4): 383–408.

Zimmerman, Matt. 2007. Testifier before the house subcommittee on elections. http://www.gpo.gov/fdsys/pkg/CHRG-110hhrg35805/pdf/CHRG-110hhrg35805.pdf. Accessed 5 Nov 2011.

Zimmermann, Philip. 1995. Author's preface to the book: "PGP Source Code and Internals". http://www.philzimmermann.com/EN/essays/index.html. Accessed 23 Oct 2011.

Zimmermann, Philip. 2001. No regrets about developing PGP. http://www.philzimmermann.com/EN/essays/index.html. Accessed 23 Oct 2011.

Chapter 4
Digital Resistance, Digital Liberties and Human Rights

4.1 Internet and Human Rights

In 1988 Bobbio, in a essay concerning the present and the future of human rights, noticed, with respect to human rights, that the serious problem of our times was not to *create* them, but to *protect* them.

The scholar outlines that it is not so much to know *which* and *how many* are these rights, which of their *nature* and their *foundation*, whether *natural* or *historical* rights, *absolute* or *relative*, but what is the safest way to protect them, to prevent, despite the solemn declarations, that are continuously violated (Bobbio 1988).

Another scholar, Forsythe, *inter alia*, has developed an interesting analysis of the evolution of human rights in the activities of the United Nations in the period before the large-scale spread of the Internet and new technologies and, in particular, in the first 40 years, from 1945 to 1985 (Forsythe 1985). The author remarks that, in the second 20 years of the United Nations activities, the situation changed markedly, and efforts increasingly moved from the *general* and the *abstract* to the *specific* and the *concrete* (some drafting efforts continued, for example, on a special instrument concerning torture). The *United Nations*, Forsythe outlines, accepted the principle of the permissibility of individual petitions and created several mechanisms to deal with them; increasingly UN bodies used publicity to *pressure* specific states and targets were not limited to South Africa and Israel, or even Chile. Finally, increasingly across the UN system, there was a fragile but persistent movement toward improved supervision of states' policies on human rights: more and more human rights treaties came into legal force and various agencies tried to see that they were implemented (Forsythe 1985: 252).

The extension of the rules for the protection of human rights *in the electronic world*, and their effective protection, is a very important topic too, and it has raised the interest of many scholars.

In this work, I will refer only to the relationship between human rights and the digital world and, deliberately, I will not explain interesting and delicate issues like

G. Ziccardi, *Resistance, Liberation Technology and Human Rights in the Digital Age*, Law, Governance and Technology Series 7,
DOI 10.1007/978-94-007-5276-4_4, © Springer Netherlands 2013

the nature of human rights and their protection; my attention will be dedicated to the assessment of the level of application of human rights to the Internet.

I think that, first of all, the world of digital resistance is closely tied to the theme of human rights essentially for three reasons:

1. the first is that the actions of digital resistance occur in states which are generally referred to as little respect for human rights, or sometimes explicitly reported or denounced. In this case, the activity of digital resistance serves also to try to highlight details on systematic violations of those rights;
2. the second reason is that a *smart* use of technology can help the expansion and the manifestation of human rights, especially freedom of expression or right to access to technology and culture, in those places where they are repressed;
3. the third reason is that there are many non-governmental associations, groups (more or less organized) and individuals who daily fight for the protection of human rights by using the Internet as a means to operate better and to make their action more effective.

Many scholars have recognized the applicability *tout court* of the protection of fundamental human rights to the electronic environment. Most importantly, moving from human rights theories and elaborating a technological research, makes it possible to establish solid bases that allow to process very articulated theories that have their roots in the great and noble legal, political and social issues of the modern era. Sartor, *inter alia*, clearly remarked this point:

> Human rights are important since they provide us with a framework for articulating some basic normative structures for the governance of the information society, in the awareness of the human values at stake. It is true, authoritative formulations, doctrinal developments and social understanding of human rights cannot provide us with a complete regulatory framework: economical and technological consideration must be taken into account, while legal traditions and political choices play a decisive role in many regards (even with regard to the very understanding of human rights and their balance). However, the human-rights discourse still play an important role: it identifies some basic fundamental needs and entitlements, it links our understanding of such needs and entitlements to successes and failures of human history, it enables us to provide a context for our analyses of the new issues emerging in the information society, linking such analyses to a rich background including legal cases as well as social, political and legal debates (Sartor 2010).

Most of the articles and principles contained in the most important statements apply peacefully to the Internet and to the activities of the users of new technologies, as they were drafted to front the technological evolution. Other scholars have analyzed citizen participation in the governance of new technologies from a human rights perspective.[1]

[1] See the study by Flear and Vakulenko concerning a human rights perspective on *citizen participation* in the EU's governance of new technologies (Flear and Vakulenko 2010). The author remark that: "The human rights perspective in the 'bioethical triangle' thus lacks clear-cut boundaries can uncertainty which is currently being explored by the burgeoning literature linking human rights to new technologies. This linkage raises the question: can citizens use human rights to connect with and help shape new technologies?" (Flear and Vakulenko 2010: 662).

At the end of an important *Expert Meeting* on human rights and the Internet held in Stockholm in 2010, chairmen remarked six fundamental issues that can be assumed as a logical starting point to analyze the complex relationship between the digital world and the human rights landscape (La Rue and Ehrenkrona 2010). These six points are:

1. *importance of the Internet in the modern age*: the Internet must be regarded as the greatest enabler for freedom of expression and other human rights since Gutenberg's printing press;
2. *challenges and risks*: the Internet poses, at the same time, challenges to the protection of human rights, perhaps most notably *the right to privacy*, as well as the legitimate interests and values of democracy;
3. *freedom, security, accessibility*: ensuring a free, secure and accessible Internet has therefore emerged not only as a fundamental human rights challenge, but as the key to global economic development, prosperity and development of Internet itself;
4. *freedom of expression as a pivotal right in the digital age*: common ground and starting point must be the reaffirmation of the fundamental right to *freedom of expression* and the need to protect this right from unlawful restrictions on the Internet: limitations of freedom on the Internet, including security-related measures, could only be acceptable if they complied with international human rights law, including existing standards of proportionality, transparency and adherence to the rule of law;
5. *new forms of human rights issues and standards*: it is important that existing human rights standards are upheld and strengthened, but the Internet also poses new challenges that need to be addressed on its own terms. Therefore, it is not sufficient to rely exclusively on existing norms, but there is need for clarification of the meaning and scope of human rights law in the Internet context;
6. *states responsibilities*: states have committed to, and are responsible for, the protection of human rights and therefore have the responsibility to address these issues.

This statement contains points of great interest, and all these six preliminary points can be useful to set a correct approach.

The authors outlines, also, that "The proliferation of sites and spaces at national, regional and international levels aimed at fostering citizen participation in the governance of science and technology demonstrates the increasing salience of citizen participation for enhancing accountability and legitimacy. In the European Union (EU), citizen participation in that governance forms part of a more general concern about tackling the 'democratic deficit' through measures that are aimed at reducing the distance between governance and citizens" (Flear and Vakulenko 2010: 663). Finally, conclusions are clear: "In talking about a human rights perspective, we take a non-doctrinal approach, paying close attention to critical theory and in particular Foucault-influenced ways of thinking about human rights, citizen participation and governance. We understand human rights to mean not just the body of law, but also the practices and projects, the 'movements or groupings of lawyers, non-governmental organizations, and others who seek to secure and defend a particular right, group of rights, or human rights in general" (Flear and Vakulenko 2010: 665).

Note, first of all, the reference to the Internet as the most important and most powerful invention since Gutenberg and printing; some scholars have even come to define it as the greatest invention since the discovery of fire. Is, then, identified the "double face" of the Internet: able to expand as much as possible human rights, especially the manifestation of the individual thought, but also able to raise large risks, including the invasion of privacy.

The first point addressed in the statement regards freedom of expression, and the approach of La Rue and Ehrenkrona is clear. First of all, the scholars remark that limitations of freedom of expression can only be permitted if compliant with international human rights standards, and such limitations should be treated as strict exceptions. The second point of discussion is that States that do regulate online content must implement *legal safeguards* to uphold transparency, strict rule of law and due process and states and companies have a common duty to make the regulations concerning online content clear and easily understandable to Internet users. With regard to filtering and blocking of online content, the authors are concerned about the possible abuse of such technology by states or companies, and therefore inclined towards allowing full control by the end user. It is then suggested a greater effort to combat illegal material, such as child-abusive images, stressing the importance of focusing on the criminals behind this material, stopping it before it got online, and warning that blocking is a blunt instrument that, in some cases, may cause adverse effects. These experts, finally, recommend that clear determinations of liability for opinions or data made available online should be defined by law and stronger protection for intermediaries should be provided, including for public access points such as cybercafés (La Rue and Ehrenkrona 2010: 1–2).

As is known, although human rights are many and involve many aspects, that of freedom of thought and expression is always cited as *the first*, even in the electronic world. The exceptional nature of the restriction of thought is seen as an indispensable ingredient. Note, in the statement, a clear reference to the world of *business* and of the *corporation*, which are capable of restricting freedom of expression and the availability of content just as authoritarian regimes.

A second aspect discussed in this study is the delicate relationship and balance between privacy and freedom of expression. The text of the *Report* about this issue recalls the importance of ensuring a positive balance between privacy and freedom of expression. The authors write that, just as the freedom of expression, privacy should be considered the baseline standard on the Internet at all levels of regulation, and, therefore, should ideally be made the default standard and be implemented by design.

The document analyses four points:

1. *anonimity*. Online anonymity was widely considered an important aspect both of the freedom of expression and of privacy, but was also deemed to have a clear limit in the liability for illegal content;
2. *criminal investigation*. Measures such as *compulsory registration* of Internet users were rejected, but further discussion regarding the technological aspects of criminal investigations is needed, within the boundaries set by the human rights framework;

3. *data encryption*. The experts also expressed scepticism about the *prohibition* of data-encryption and circumvention techniques. Such a prohibition, they argued, would have a clear "chilling effect" on the freedoms of information and expression and may have a negative impact on the shaping and the further development of the Internet. On the other hand, only openness and the limitation of restrictions to a necessary minimum could prevent encryption from evolving into a new standard;
4. *data retention*. Experts believed that the right to privacy further argued in favour of reducing data retention by states and companies to a minimum. It was argued that more direct user control over personal data was needed, highlighting the importance of strengthening the implementation of fundamental human rights principles such as transparency, rule of law and due process. Governments and businesses shared the duty to inform and educate the public about the use of personal data (La Rue and Ehrenkrona 2010: 2).

The final point of the Report, with reference to human rights, concerns the right to access to the Internet and is also very interesting. The authors explain that access to the Internet was thoroughly examined from a human rights perspective, and it was widely considered to be a principle of human rights law and an enabler for several other human rights too. Many arguments were brought forth as to the civil and political, as well as to the social and economical aspects of the right to access; the notion that the right to access was *of less importance* to the 'developed world' was dispelled, although it was noted that the 'developed world' perhaps stood at a different point in the trajectory of access compared to developing nations. Access to Internet thus needed to be addressed both as (i) access to the medium, in terms of technology, and (ii) as access to content and the right to speak. States needed not only limit the restrictions of online content, but also make efforts to promote access to the medium (La Rue and Ehrenkrona 2010: 3–4).

Sartor, concerning this issues, identifies eight points that are a clear evidence of the importance of the Internet for human rights (Sartor 2010: 2–4). These points are:

1. ICTs provide many new opportunities for *economic development* and enable a vast increase in productivity, in industrial production as well all in related administrative and commercial processes;
2. ICTs can contribute to the *efficiency* in public organisations, reducing the administrative costs involved in delivering public services, and providing more information, transparency and accountability, so favouring equal access. Workflows can be redesigned and accelerated, mechanical activities can be automated, citizens' interactions with the administration can be facilitated, documents can be made publicly accessible, participation in administrative proceedings can be enhanced, and so can controls over the exercise of administrative and political functions;
3. ICTs can contribute to deliver information, education and knowledge to everybody;
4. ICTs deliver unprecedented opportunities for individual creativity;
5. ICTs enable the aggregation of individual efforts into social knowledge;

6. information technologies enable individuals to interact with their peers, regardless of physical distance;
7. ICTs (and in particular the Internet) have enabled the formation of a new public sphere, where individuals merge their opinions and build social knowledge in a variety of ways;
8. ICT may favour moral progress: by overcoming barriers to communication, offering people new ways of collaboration, reducing costs involved in engaging in creative activities, it may favour attitudes inspired to universalism, (reasonable) altruism, and participation, beyond what may be expected from a merely self-interest person.

All those eight aspects are strictly related to the human rights "level" in several countries.

4.2 Internet and the *Universal Declaration of Human Rights*

Moving from the crucial document *The Universal Declaration of Human Rights* (UDHR), adopted by the United Nations General Assembly the 10 of December 1948, it is possible to bring together the principles that are related to digital resistance actions that take place in countries where human rights are violated.

Giving a sort of "technological interpretation" to this historic document, it seems appropriate to bring together the principles in *eight* areas very interesting for the technological world and the digital dissidents framework:

1. all those principles that provide a *general prohibition of discrimination* in any (including online) activities. In this first category fall the statements of Article 1,[2] Article 2[3] and Article 3.[4] These principles apply to the digital world in a variety of situations. Equal dignity and rights mean, first of all, *equal right of access to the Internet* and information assets. Discrimination based on religion, politics and gender prevent then, even online, a free expression of freedom. Finally, the differences in jurisdictional situation affect much Internet presence;

[2] The text of Article 1 of the UDHR is: "All human beings are born free and equal in dignity and rights. They are endowed with reason and conscience and should act towards one another in a spirit of brotherhood".

[3] The text of Article 2 of the UDHR is: "Everyone is entitled to all the rights and freedoms set forth in this Declaration, without distinction of any kind, such as race, colour, sex, language, religion, political or other opinion, national or social origin, property, birth or other status. Furthermore, no distinction shall be made on the basis of the political, jurisdictional or international status of the country or territory to which a person belongs, whether it be independent, trust, non-self-governing or under any other limitation of sovereignty".

[4] The text of Article 3 of the UDHR is: "Everyone has the right to life, liberty and security of person".

2. all those principles which establish the right not to be *discriminated by the authority*, threatened or suffer degrading treatment. These statements are included in Article 5,[5] in Article 9,[6] in Article 12[7] and in Article 29.[8] It is known that the indiscriminate arrest, torture and an instrumental use of the judicial system are often used to *silence* independent news, citizen journalists and blogger. Even the imprisonment in facilities that put a strain on the health of the prisoner, or the inability to exit the country or to return, because of the political views expressed;
3. those principles which include the right not to be discriminated by the *judicial system*. In particular, I refer to Article 8[9] and Article 11[10];
4. those principles that protect freedom of expression. I refer in particular to Article 10[11];
5. those principles protecting freedom of movement, and in particular Article 13[12] and Article 14[13];

[5] The text of Article 5 of the UDHR is: "No one shall be subjected to torture or to cruel, inhuman or degrading treatment or punishment".

[6] The text of Article 9 of the UDHR is: "No one shall be subjected to arbitrary arrest, detention or exile".

[7] The text of Article 12 of the UDHR is: "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks".

[8] The text of Article 29 of the UDHR is: "(1) Everyone has duties to the community in which alone the free and full development of his personality is possible. (2) In the exercise of his rights and freedoms, everyone shall be subject only to such limitations as are 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. (3) These rights and freedoms may in no case be exercised contrary to the purposes and principles of the United Nations".

[9] The text of Article 8 of the UDHR is: "Everyone has the right to an effective remedy by the competent national tribunals for acts violating the fundamental rights granted him by the constitution or by law".

[10] The text of Article 11 of the UDHR is: "(1) Everyone charged with a penal offence has the right to be presumed innocent until proved guilty according to law in a public trial at which he has had all the guarantees necessary for his defence. (2) No one shall be held guilty of any penal offence on account of any act or omission which did not constitute a penal offence, under national or international law, at the time when it was committed. Nor shall a heavier penalty be imposed than the one that was applicable at the time the penal offence was committed".

[11] The text of Article 10 of the UDHR is: "Everyone is entitled in full equality to a fair and public hearing by an independent and impartial tribunal, in the determination of his rights and obligations and of any criminal charge against him".

[12] The text of Article 13 of the UDHR is: "(1) Everyone has the right to freedom of movement and residence within the borders of each state. (2) Everyone has the right to leave any country, including his own, and to return to his country".

[13] The text of Article 14 of the UDHR is: "(1) Everyone has the right to seek and to enjoy in other countries asylum from persecution. (2) This right may not be invoked in the case of prosecutions genuinely arising from non-political crimes or from acts contrary to the purposes and principles of the United Nations".

6. those principles governing the freedom of thought and of peaceful assembly, and in particular Article 18,[14] Article 19[15] and Article 20[16];
7. those principles that apply in critical periods such as the elections, and I refer to Article 21.[17] Concerning this point, the scholar Saul, *inter alia*, outlined very well the violence and the human rights violations occurring during parliamentary elections moving from the Sri Lanka example (Saul 2002) and the violation of the international right to a free and fair election. Saul notes that election violence was politically motivated, rather than based on race, ethnicity or religion, and that political violence also strikes the integrity of the democratic process: it is a crime against deliberation and dialogue, against participation and peaceful means of settling disputes. Last, but not least, political violence also infringes on a constellation of specific human rights: rights to life, bodily integrity, liberty, freedom of opinion, expression and association, to vote and freely choose elected representatives, property and not to leave in fear (Saul 2002: 3). Bloggers usually report the three phases of election related violence (Saul 2002: 25): (i) pre-election violence, (ii) election day violence, and (iii) post-election violence, the misuse of state resources for party political purposes and ballots/polling stations regularity before the result is presented;
8. those principles governing the freedom of culture and knowledge, and in particular Article 26[18] and Article 27.[19] The need for access to information is fundamental

[14] The text of Article 18 of the UDHR is: "Everyone has the right to freedom of thought, conscience and religion; this right includes freedom to change his religion or belief, and freedom, either alone or in community with others and in public or private, to manifest his religion or belief in teaching, practice, worship and observance".

[15] The text of Article 19 of the UDHR is: "Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers".

[16] The text of Article 20 of the UDHR is: "(1) Everyone has the right to freedom of peaceful assembly and association. (2) No one may be compelled to belong to an association".

[17] The text of Article 21 of the UDHR is: "(1) Everyone has the right to take part in the government of his country, directly or through freely chosen representatives. (2) Everyone has the right of equal access to public service in his country. (3) The will of the people shall be the basis of the authority of government; this will shall be expressed in periodic and genuine elections which shall be by universal and equal suffrage and shall be held by secret vote or by equivalent free voting procedures".

[18] The text of Article 26 of the UDHR is: "(1) Everyone has the right to education. Education shall be free, at least in the elementary and fundamental stages. Elementary education shall be compulsory. Technical and professional education shall be made generally available and higher education shall be equally accessible to all on the basis of merit. (2) Education shall be directed to the full development of the human personality and to the strengthening of respect for human rights and fundamental freedoms. It shall promote understanding, tolerance and friendship among all nations, racial or religious groups, and shall further the activities of the United Nations for the maintenance of peace. (3) Parents have a prior right to choose the kind of education that shall be given to their children".

[19] The text of Article 27 of UDHR is "(1) Everyone has the right freely to participate in the cultural life of the community, to enjoy the arts and to share in scientific advancement and its benefits. (2) Everyone has the right to the protection of the moral and material interests resulting from any scientific, literary or artistic production of which he is the author".

to inform populations of their rights as individuals, and often the information is deleted just to ensure that rights are not known.

4.3 The Council of Europe and the Human Rights Guidelines for Internet Service Providers: The Role of ISPs in Human Rights Environments and Protection

According to the Council of Europe, in a document including human rights guidelines for Internet Service Providers (ISPs), these companies, in providing the basic infrastructure and the basic services that allow users to access and use the Internet and, thereby, exercise their rights to benefit from the information society, deliver services with a significant public service value to society.

These companies have a unique position and possibility of promoting the exercise of, and respect for, human rights and fundamental freedoms and, in addition, the provision of Internet services is increasingly becoming a prerequisite for a comprehensive *participatory democracy*.

ISPs also play an important role in those states which are committed to protecting and promoting these rights and freedoms as part of their international law obligations: access-providers, for example, facilitate entry to the Internet and therefore to a diversity of information, culture and languages; they are often the first point of contact and trust for users.

Their role is so a prerequisite for enabling and empowering users to access the benefits of the information society, in particular to seek and impart information and ideas, to create and to access knowledge and education.

Equally, to the extent that access-providers, and particularly host-providers, may enforce decisions and actions with regard to the accessibility of services (i.e. remove, block or filter content), this can impact on rights and freedoms.

ISPs have access to varying amounts of information (content and/or traffic data) which underlines their important role and position in front of the rights and freedoms of users. ISPs should not be put under a general obligation to actively monitor content and traffic data; however there may be specific cases defined by law and upon specific orders where an ISP may need to assist in monitoring content or data or impart information about a user to a third party. Such cases could have an impact on freedom of expression or the right to private life.

Nine main points are remarked in these guidelines:

1. ISPs must make sure that any filtering or blocking of services carried out is (a) legitimate, (b) proportional, and (c) transparent to customers in accordance with the Council of Europe Recommendation on measures to promote the respect for freedom of expression and information with regard to Internet filters, CM/Rec (2008);
2. ISPs must *inform* customers of any filtering or blocking software installed on their servers that may lead to a removal or inaccessibility of content as well as the

nature of the filtering that takes place (form of filtering, general criteria used to filter, reasons for applying filters);
3. ISPs, in respect of filtering, blocking or removal of illegal content, should do so only after a verification of the illegality of the content, for instance by contacting the competent law enforcement authorities;
4. ISPs acting without first checking and verifying may be considered originating an interference with legal content and with the rights and freedoms of those creating, communicating and accessing such content, in particular the right to freedom of expression and information;
5. ISPs, when acting with regard to the communications of users (for example: by allowing the interception or monitoring of users' e-mails), should undertake that action only in case of a legal duty to do so, on specific orders or instructions from a competent public authority made in accordance with the law;
6. ISPs do not have to actively monitor the content of communications on the network. Furthermore, the deletion and modification of the user's correspondence (e.g. by spam-filters) should depend on the explicit consent of the user before the spam-filter is activated;
7. ISPs must not reveal the identity of users, their traffic data or the content of data accessed by them to a third party, unless under a legal duty to do so or following specific orders or instructions from the competent public authority made in accordance with the law. Requests in this respect brought from abroad should be handled through the competent authorities in the country where the ISPs operate;
8. ISPs must inform their customers in which circumstances the provider is under a legal duty to reveal their identification, connection or traffic data by request from law enforcement agencies;
9. ISPs, if receive a request to disclose such data, must make sure to check the authenticity of the request and that it is made by a competent authority in accordance with the law.

4.4 The WSIS Declaration of Principles

The first *United Nations World Summit on the Information Society* (WSIS), held in December 2003, recognized too the connections between information technology and human rights with a *Declaration of Principles* (*Building the Information Society: a global challenge in the new Millennium*), a sort of "Constitution for cyberspace" that called for the development of the information society to conform to recognized standards of human rights.[20]

[20] See the text at the address http://www.itu.int/wsis/docs/geneva/official/dop.html. Accessed 13 November 2011.

There are numerous points of this statement that relate, directly or indirectly, to human rights.

The first point, included in the premises, it is very clear: is an explicit reference to the *Universal Declaration of Human Rights* and declares a common desire and commitment to build a people-centred, inclusive and development-oriented Information Society, where everyone can create, access, utilize and share information and knowledge, enabling individuals, communities and peoples to achieve their full potential in promoting their sustainable development and improving their quality of life. This hope is premised on the purposes and principles of the Charter of the United Nations and respecting fully and upholding the Universal Declaration of Human Rights.

The following points of the document, 2 and 3, deal with the very delicate themes of poverty and hunger, education, minorities and health.

In this case the challenge states are facing is to harness the potential of information and communication technology to promote the development goals of the Millennium Declaration, namely the eradication of extreme poverty and hunger; achievement of universal primary education; promotion of gender equality and empowerment of women; reduction of child mortality; improvement of maternal health; to combat HIV/AIDS, malaria and other diseases; ensuring environmental sustainability; and development of global partnerships for development for the attainment of a more peaceful, just and prosperous world.

Consequently, the authors of the document reaffirm the universality, indivisibility, interdependence and interrelation of all human rights and fundamental freedoms, including the right to development, as enshrined in the Vienna Declaration, and that democracy, sustainable development, and respect for human rights and fundamental freedoms as well as good governance at all levels are interdependent and mutually reinforcing.

An explicit reference to the Article 19 and to the Article 29 of the Universal Declaration oh Human Rights is contained in point 4 and 5 of the document. Namely, the authors of the document reaffirm, as an essential foundation of the Information Society, and as outlined in Article 19 of the Universal Declaration of Human Rights, that *everyone has the right to freedom of opinion and expression*; that this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers.

Communication, is remarked, in this document, is a fundamental social process, a basic human need and the foundation of all social organization, and it is central to the Information Society. Everyone, everywhere should have the opportunity to participate, and no one should be excluded from the benefits the Information Society offers.

A second, fundamental point is the reaffirmation of the commitment to the provisions of Article 29 of the Universal Declaration of Human Rights, stating that everyone has duties to the community in which the free and full development of their personality is possible, and that, in the exercise of their rights and freedoms, everyone shall be subject only to such limitations as are 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. These rights and freedoms may in no case be exercised contrary to the purposes and principles of the United Nations, and in this way, must be promoted an Information Society where human dignity is respected.

Digital divide and developing countries, particularly vulnerable groups and indigenous peoples are to be protected within the meaning of points 10, 13, 14, 15 e 16.

In this portion of the document, five important issues are described:

1. *digital divide*. There must be the awareness that the benefits of the information technology revolution are today unevenly distributed between the developed and developing countries and within societies.[21] The project must be to turning this digital divide into a *digital opportunity* for all, particularly for those who risk being left behind and being further marginalized;
2. *protection of marginalized and vulnerable groups*. In building the *Information Society*, everyone shall pay particular attention to the special needs of marginalized and vulnerable groups of society, including migrants, internally displaced persons and refugees, unemployed and underprivileged people, minorities and nomadic people, and also recognize the special needs of older persons and persons with disabilities;
3. *empowerment of the poor*. There is the necessity, and the explicit will of the political system, to empower the poor, particularly those living in remote, rural and marginalized urban areas, to access information and to use new technologies as a tool to support their efforts to lift themselves out of poverty;
4. *preservation of heritage and cultural legacy*. In the evolution of the *Information Society*, particular attention must be given to the special situation of indigenous peoples, as well as to the preservation of their heritage and their cultural legacy;
5. *attention to countries in transition or in particular critical conditions*. Special attention must be payed to the particular needs of people of developing countries, countries with economies in transition, least developed countries, small island developing states, landlocked developing countries, highly indebted poor countries, countries and territories under occupation, countries recovering from conflict and countries and regions with special needs as well as to conditions that pose severe threats to development, such as natural disasters.

The last remarks of our interest in the document (18, 55, 58 and 59) refer to topical points too. The principles of freedom of the press and freedom of information, as well as those of the independence, pluralism and diversity of media, are remarked as essential to the Information Society. The same with freedom to seek, receive, impart and use information for the creation, accumulation and dissemination of knowledge, similarly important to the Information Society.

The document call for the responsible use and treatment of information by the media in accordance with the highest ethical and professional standards: traditional media in all their forms have an important role in the Information Society and ICTs should play a supportive role in this regard. Diversity of media ownership

[21] See Sect. 1.4.

should be encouraged, in conformity with national law, and taking into account relevant international conventions.

The authors reaffirm also the necessity of reducing international imbalances affecting the media, particularly as regards infrastructure, technical resources and the development of human skills.

Finally, the use of ICTs and content creation should respect human rights and fundamental freedoms of others, including personal privacy, and the right to freedom of thought, conscience, and religion in conformity with relevant international instruments. All actors in the Information Society should take appropriate actions and preventive measures, as determined by law, against abusive uses of ICTs, such as illegal and other acts motivated by racism, racial discrimination, xenophobia, and related intolerance, hatred, violence, all forms of child abuse, including paedophilia and child pornography, and trafficking in, and exploitation of, human beings.

4.5 The 2011 United Nations Report on the Promotion and Protection of the Right to Freedom of Opinion and Expression

The report of the United Nations (UN Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue, United Nations Human Rights Council, May 16, 2011) I'm going to examine in detail has the advantage of cover, with great clarity, the delicate relationship between the protection of human rights worldwide and the close relationship with the new technologies.

In addition to highlight normative references and behaviors typical of breaches of human rights, offers suggestions that can help improve the bleak picture that is drawn, and also take into consideration the limits of freedom of expression and the protection of rights.

The aim of the Report is well indicated in the Summary, and it is not only exploratory, but aims to detect some benchmarks about the applicability of the principles and norms relating to human rights to the technology environment, highlighting the exceptional cases which may allow a limitation.

The points that are highlighted are, in my opinion, very interesting.

The first is the right for every individual to seek, receive and impart information and ideas of all kinds on the Internet. The Internet not only allows to exercise fundamental right to freedom of opinion and expression, but also a much wider range of human rights and to promote the progress of society as a whole. Appears obvious, then, the applicability of international human rights law and standards usually referred to the right of opinion and expression also to the Internet, intended as a means of communication.

An interesting part of the report is the one that lays down the exceptional circumstances under which the dissemination of a certain type of information may be limited.

Are explained two dimensions of Internet access: (i) access to content, and (ii) access to the physical and technical infrastructure that require access to the Internet and that are preliminary to the possibility of access to content. Finally, are described the typical ways in which States are increasingly censoring the Internet and information online, through the arbitrary blocking or filtering of content, the criminalisation of legitimate expressions, the imposition of liability of the provider to disconnect users from the Internet according to the law on intellectual property, cyber-attacks and low protection of the right to privacy and data.

The first point of interpretation addressed in the Report, of great interest for the jurist, concerns the applicability or not of the principles of Article 19 of the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights to the use of the Internet by users and the fact that the Internet has become an essential means through which individuals exercising their right to freedom of expression.

The author of the Report points out, first, principles contained in article 19, and extends them to the electronic environment, since the Internet has become a key medium through which individuals can exercise their rights of freedom of expression and opinion. The article 19 was, however, thought having regard also to the technologies of the future:

(a) Everyone shall have the right to hold opinions without interference;
(b) Everyone shall have the right to freedom of expression; this right shall include freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of his choice;
(c) The exercise of the rights provided for in paragraph 2 of this article carries with it special duties and responsibilities. It may therefore be subject to certain restrictions, but these shall only be such as are provided by law and are necessary;
(d) for respect of the rights or reputations of others;
(e) for the protection of national security or of public order (ordre public), or of public health or morals.

The great potential of the Internet communication has raised fears soon in many Governments about the controllability of this huge information flow, and this fear has led to reactions that put in danger, and in discussion, the principles of article 19. On the one hand there is the awareness of the centrality of the right of expression in the electronic world, on the other hand a clear reaction by many centres of power in an attempt to control these liberties. The right to freedom of opinion and expression is a fundamental right in itself, and is a right which is prerequisite for the full implementation of other rights like economic, social and cultural rights such as the right to an education, to be a part of cultural life, to benefit from scientific advances, and civil and political rights, such as the assemble peaceably. This, combined with the speed of the medium and the possibility of a relative anonymity, scares governments and leads to restrictions with increasingly sophisticated technologies.

An interesting part of the report concerns the applicability of paragraph 3 of article 19 to the restriction of liberty. There are, in particular, certain types of expression that can be legitimately limited by States according to the laws on human rights.

It offers a cumulative test, in three parts to see if these restrictions are legitimate:

1. It must be provided by law, which is clear and accessible to everyone (principles of predictability and transparency);
2. It must pursue one of the purposes set out in article 19, paragraph 3, of the Covenant, namely (i) to protect the rights or reputations of others, or (ii) to protect national security or of public order, or of public health or morals (principle of legitimacy);
3. It must be proven as necessary and the least restrictive means required to achieve the purported aim (principles of necessity and proportionality). Moreover, any legislation restricting the right to freedom of expression must be applied by a body which is independent of any political, commercial, or other unwarranted influences in a manner that is neither arbitrary nor discriminatory, and with adequate safeguards against abuse, including the possibility of challenge and remedy against its abusive application.

The result of an interpretation so strict limits which restrict the freedom of expression, to identify the types of content that may be subject to such strict limitations, for example child pornography, or to protect the rights of children, expressions of hatred, defamation to protect reputation, direct and public incitement to commit genocide, racial hate, violence. A concrete problem, though, is that these limits are not always respected, and actions to limit the content do not rely on policy so rigid (and guaranteed) but most are based on discretion, often flawed, of rulers. There are often legal basis thus defined in advancing shares content restriction, but with ambiguous rules or too vague and broad, or disproportionate in their sanctions, and these rules also lead to self-censorship.

The conclusion is that it must be clear the conditions and criteria on which the restriction of freedom of expression. Any restriction of the right to freedom of expression must adhere to rigid standards of international human rights standards, especially when used the criminal law, which also leads to physical violence against persons and degrading treatments.

The report outlines several point regarding practical methods of human rights violations. These methods are:

1. *Arbitrary blocking or filtering of content*. The block of content, i.e. to make impossible for a user to reach a specific content, or for a particular content to reach a user, is one of the most common methods to limit the rights of expression and knowledge, and an interesting point is that many blocking or filtering systems are kept hidden. The Report illustrates typical techniques through which are carried out these activities, and the consequences. These actions range from preventing user access to a specific site, IP addresses, domain extensions, take down web sites from the web server where they are hosted, use filtering technologies

for certain pages or sites that contain keywords. Interesting is also the increasingly widespread of phenomena like the block "just in time", on the occasion of certain political events such as elections, anniversaries or to popular unrest, and the complete disconnection from the Internet (Internet shut-down). The consequences of such behaviour from a regulatory point of view, and with reference to the articles mentioned above, are clear. Often the block is not guaranteed by a law, but vague, and therefore allows an arbitrary and excessive use of this system. More, it usually prevents the vision of legitimate contents;

2. *Criminalization of Legitimate Expression*. A second point of aggression to human rights does not target the so-called end users, trying to keep them away from the content, but targets directly the person who, for example, is doing political activity in authoritarian areas using arrest, imprisonment, violence and silencing dissonant voices. The physically muting of criticism and dissent with arrests and detentions, forced disappearances, intimidation and violence, is an old phenomenon that also applies to the Internet. These actions serve also to intimidate the rest of the population, and usually rely on the protection of reputation, on the pretext of terrorism, national security to, in practice, serve to censor unwelcome content. Arrest of bloggers in the world are a typical result of these actions;
3. *Imposition of intermediary liability*. In this case the target are intermediaries or, better, the target is the system of the Internet and its operativity, and is a very easy way to limit the exercise of rights. Law regarding ISPs, search engines providers, blogging platforms, or other services, and promoting intervention on these systems, may limit the freedom (at the beginning of the Internet era, the reason why these services flowered and changed the face of the Internet was, also, keeping them free from an objective responsibility). However this is not always so, today, and this immunity is a little misleading. Many States have adopted laws that impose liability for intermediaries if they don't filter or block contents, or if they don't block some types of users. Turkey, for example, Thailand and the judgment of Google[22] in Italy, but also in China, are clear examples of big risks (and the risk is often not only prison, but also the withdrawal of the ISP license). The report also discusses, concerning this point, the notice-and-take-down regime, a framework that exists in many States and that requires the reaction of the providers as soon as they are told they must remove a specific content. It is true that a similar process protects intermediaries from liability, but is also a tool that can easily be used as a method of censorship or to generate responsibility. A useful starting point is the EU directive on e-commerce, for which an ISP is not responsible if do not has current knowledge of the content and illegal activity and promptly removes it as soon as it is notified or becomes aware. However, this system can be clearly abused either by the State or by private actors (if there are sanctions, in doubt the provider removes the content);

[22] See the Sartor and Viola de Azevedo Cunha study regarding the Italian Google case and the conviction of three Google executives for violating the Italian data protection law (Sartor and Viola de Azevedo Cunha 2010).

4. *Disconnecting Users from Internet Access*. Several States have also taken steps to cut the connection to the Internet, and to disconnect users if they violate intellectual property rights. In France, for example with a graduated, three strikes action, and in the United Kingdom;
5. *cyber-attacks*. Attacks on computers, hacking and denial-of-service actions are usually taken during very important political unrest. Also web sites of human rights and dissidents are often targeted. If such attacks come from a state or a government, certainly violate the obligation to respect the freedom of expression. In any case, States must protect its citizens from such attacks and investigate in this sense. In a topical study concerning these issues, Zuckerman, Roberts, McGrady, York and Palfrey analyzed distributed denial of service attacks against independent media and human rights sites. These scholars remarks the following fundamental statements (Zuckerman et al. 2010: 3–4): (a) DDoS attacks against independent media and human rights sites have been common in the past years, even outside of elections, protests, and military operations. With recent highly publicized DDoS attacks on Wikileaks, and "Operation Payback" attacks by "Anonymous" on sites perceived to oppose Wikileaks, the scholars expect these attacks to become more common; (b) independent media and human rights sites suffer from a variety of different types of cyber attacks, including filtering, intrusions, and defacements in addition to DDoS attacks, and those attacks interact with each other in complex ways; (3) independent media and human rights sites suffer from both application DDoS attacks, which exhaust local server resources and can usually be mitigated by a skilled system administrator; and network DDoS attacks, which exhaust network bandwidth and can usually only be mitigated with the help of a hosting provider at considerable expense; (5) Mitigating DDoS attacks against independent media and human rights sites will likely require moving those sites closer to the core of the Internet: inside the small number of major ISPs, websites, and content distribution networks (CDNs) that have the experience and resources to defend against these attacks, particularly network DDoS attacks. These scholars, finally, recommend the following responses to DDoS attacks against independent media and human rights sites: (1) Application attacks can be strongly mitigated by replacing complex content management systems (CMSes) with static HTML or by adding aggressive caching systems to deliver content at the expense of interactivity; (2) All organizations should carefully consider whether to host their sites on a free, highly DDoS- resistant hosting service like Blogger, even at the cost of prestige, functionality and possible intermediary censorship. Organizations that choose to host their own sites should plan for attacks in advance, even if those plans include acceptable levels of downtime; (c) Organizations that choose to host their own sites should use systems to detect attacks and, when necessary, degrade site performance and retreat to backup hosting on a free, highly DDoS-resistant hosting service like Blogger. Simple modules for popular content management systems could automate this process and minimize the disruption of an attack; (d) Human rights funders should identify and support local experts in communities of the attack sites, since defending against DDoS and other attacks requires not only technical

skill but also knowledge about and trust of each of the local communities; (e) Human rights funders should consider funding a coordinator to identify both local experts for human rights communities and core network organizations willing to help human rights sites and to help local experts and core networks organizations work with one another; (f) The human rights community should work with Internet service providers (ISPs) and online service providers (OSPs) to identify providers who will work to protect sites from DDoS and who will agree not to remove controversial content unless required by law; (g) the scholars propose a broad public discussion of a range of policy responses to the rise of DDOS attacks against independent media organizations and human rights groups, with a view toward a sustainable long-term approach that balances the range of legitimate interests involved. Another scholar, Nazario, regarding politically motivated denial of service attacks (Nazario), remarks that DDoS attacks are crippling because they are designed to make the networks they target unusable, either to inflict damage to the victim or, in the case of many recent events, to silence their opponents by making their resources inaccessible. The scholar outlines how DDoS attacks provide a simple, easily available mechanism to disrupt the Internet presence of a group or a small nation. Previously, they have been confined to retaliatory attacks seeking punitive damage to the victim, but in recent years the role of the Internet in publishing newspapers or organizing dissident efforts has grown. The growing importance of the Internet to potential victims has not escaped cyberwar practitioners, and, the scholar remarks, DDoS attacks will continue as a tool of censorship as long as the Internet remains a communications medium. Nazario notes also that Cyber-warfare takes on different forms in different areas of the world. Political targets and motivations in DDoS attacks are most popular in Russia and the region, less so in China, Asia and the Middle East. China favors more surgical, infiltration events for serious cyber warfare. He observes an explosion of DDoS tools from Chinese hackers, although most of their targets are commercial sites located in China, but many are in South Korea or Japan. These sites are the targets of bullying or extortion attacks that do not yet rise to the level of political warfare. Burma benefits from website defacements and destruction. Israel and Palestine often use website defacements to challenge each other. At this time we expect to see DDoS attacks continue to be a political weapon in the Russian power sphere, particularly for former Soviet bloc nations. These attacks will continue to provide the nation-state benefits from their actions as well as plausible deniability should they actively engage in such actions. Because of this the scholar expect their frequency to grow in the Russian region, together with their sophistication as victims begin to develop improved defenses. Furthermore he anticipate that other nations may begin using DDoS attacks as a simple, blunt force political weapon to silence critics or opponents;

6. *Inadequate Protection of the Right to Privacy and Data Protection*. The right to privacy is essential to ensure that individuals can express themselves freely, as well as important is the possibility to discuss anonymously, especially on sensitive topics. On the other hand, States and individuals can collect information and data to identify individuals by restricting the flow of ideas. The pretext of national

security or protection from terrorism is very used to restrict the policy, but sometimes it is done for political or investigative purposes (the use of Facebook to investigate undercover or to track users). Also the obligation of *a real name* to gain access to the Internet, or the prohibition on the use of cryptographic systems, are indirect methods for violating the privacy of the subject but with sensitive effects. There is also a need of clarity on data retention laws and on how long the data should be kept.

The document outlines a second, fundamental problem, regarding the obligation of States to draft certain policies that favour the development of infrastructure and to guarantee universal access to the Internet, and avoid the digital divide, because digital divide entails a disadvantage for those who can't attend and cannot make their voices heard and, as a consequence, people can not use a great educational tool.

Conclusions are clear: having regard to the capacity of the Internet to improve people's lives, helping individuals to receive information and ideas in a cheap, and make the best use of their freedom, it is necessary to keep to a minimum regulation. There must be less restriction to the flow of information in the Internet and block must occur in only exceptional circumstances laid down by international law on human rights. The full guarantee of freedom of expression must be the norm. Each limitation, an exception. The restriction of online content must follow in part the content offline and still must be imposed as an exceptional measure. Should pass a cumulative three-part test: it must be laid down by law, which must be clear and accessible to all; must be done on one of the purposes referred to in art. 19, paragraph 3, of the Covenant on Civil and Political Rights, for example to protect the reputation of others, national security, public order, health and must be proven that is required and must be less restrictive means to achieve the goal. In addition, any law that requires removal, must be imposed by an independent body. An accurate control system blocking, unknown and very often transparent to users and used for purposes of censorship. See if they are really needed. The decision of what to block and block it should be taken by a court or by an independent body. Justified the measures on child pornography but we must also strengthen the traditional investigative strategies.

About the criminalisation of legitimate expression, greater attention to the crime of defamation, and do not use the excuses of terrorism or national security to restrict expression. Concerning the responsibility of the provider, never delegate the censorship measures to private entities, and intermediaries should never be blamed if they refuse to take measures contrary to human rights. Every request to an ISP to reveal user data must be made by a court, or by an independent body, and also must help corporations to respect human rights. Users must be able to appeal, and also transparency on the part of ISPs is important: a good action could be to make public requests that arrive. Disconnect users from access is seem as disproportionate, and also Cyber attacks against organizations for the protection of human rights critics, bloggers or individuals who disseminate information if they are made by States are a clear violation of the rights of freedom of expression; if they are made by private individuals is the obligation of the State to protect its citizens and to investigate.

Last but not least, regarding provacy, main issues are the respect of anonymity and encryption and the prohibition of systematic collecting of user data.

4.6 A Charter of Human Rights and Principles for the Internet

The *Charter of Human Rights and Principles for the Internet* has been developed by the *Dynamic Coalition on Internet Rights and Principles*, builds on the WSIS Declaration of Principles of Geneva and the Tunis Agenda for the Information Society, which both recognize that Information Communication Technologies (ICTs) present tremendous opportunities to enable individuals, communities and peoples to achieve their full potential in promoting their sustainable development and improving their quality of life. Like the WSIS Declaration, the Charter aims at building a people-centered information society, which respects and upholds fundamental human rights that are enshrined in the Universal Declaration of Human Rights (UDHR).

The Charter interprets and explains universal human rights standards in a new context – the Internet – and re-emphasizes that human rights apply online as they do offline: human rights standards, as defined in international law, are non-negotiable. The Charter also identifies Internet policy principles which are necessary to fulfill human rights in the Internet age – to support and expand the capacity of the Internet as a medium for civil, political, economic, social and cultural development. There are several interesting points in this document:

1. *Access to the Internet*. The first point is the right to access to the Internet, according which everyone must have the right to access to, and make use of, the Internet. The right to access to the Internet includes three fundamental aspects: (1) *Quality of service* (the quality of service to which people are entitled access shall evolve in line with advancing technological possibilities), (2) *Freedom of choice of system and software use* (access includes freedom of choice of system, application and software use, and to facilitate this and to maintain interconnectivity and innovation, communication infrastructures and protocols should be interoperable, and standards should be open, and everyone should be able to innovate in content, applications, and services without having to undergo centralized authorization and validation procedures), (3) *Ensuring digital inclusion* (digital inclusion requires that all people have access to, and effective use of, the range of digital media, communication platforms and devices for information management and processing, and to this end active support shall be available for self-managed and other community-based facilities and services, public Internet access points shall be made available, such as at telecentres, libraries, community centers, clinics and schools, and access to the Internet via mobile media must also be supported), (4) *Net neutrality and net equality* (The Internet is a global commons, and its architecture must be protected and promoted for it to be a vehicle for free, open, equal and non-discriminating exchange of information, communication and culture, and there should be no special privileges for, or obstacles against, any party

or content on economic, social, cultural, or political grounds), (5) Right to non discrimination in Internet access, use and governance. It means, essentially, equality of access (certain groups in society systematically have more limited or restricted Internet access and the means and opportunities for effective use than others, and this can amount to de-facto discrimination in terms of their ability to enjoy the human rights that the Internet supports), marginalized groups (the specific needs of all people in using the Internet must be addressed as part of their entitlement to dignity, to participate in social and cultural life, and to respect for their human rights, and special attention must be paid to the needs of marginalized groups including the elderly, young people, ethnic and linguistic minorities, and indigenous peoples, persons with disabilities and all sexuality and gender identities. All hardware, code, applications and content should be designed using universal design principles so that they are usable by all people, to the greatest extent possible, without the need for adaptation or specialized design, and this includes the need for multiple languages and scripts to be supported), and gender equality (women and men have an equal right to learn about, define, access, use and shape the Internet, and there must be full participation of women in all areas related to the development of the Internet to ensure gender equality);

2. *Right to Liberty and Security on the Internet*. This point deals with the protection against all forms of crime (everyone shall be protected against all forms of crime committed on or using the Internet including harassment, cyber-stalking, people trafficking and misuse of one's digital identity and data) but also with the security of the Internet (everyone has the right to enjoy secure connections to and on the Internet, and this includes protection from services and protocols that threaten the technical functioning of the Internet, such as viruses,[23] malware and phishing);

[23] In 2012 Goodin, moving from a Symantec study, reported (Goodin 2012) about an espionage software, in Iran, that was recently found targeting Iranian computers and that contains advanced Bluetooth capabilities, taking malware to new heights by allowing attackers to physically stalk their victims. The Author remarks: "The Flame malware, reported earlier this week to have infiltrated systems in Iran and other Middle Eastern countries, is so comprehensive that security experts have said it may take years for them to fully document its inner workings. In a blog post published Thursday, Symantec researchers dangled an intriguing morsel of information concerning one advanced feature when picking apart a module that the binary code referred to as BeetleJuice. The component scans for all Bluetooth devices in range and collects the status and unique ID of each one found, presumably so that it can be uploaded later to servers under the control of attackers […] It also embeds an encoded fingerprint into each infected device with Bluetooth capabilities. The BeetleJuice module gives the attackers the ability to track not only the physical location of the infected device, but the coordinates of smartphones and other Bluetooth devices that have been in range of the infected device. This will be particularly effective if the compromised computer is a laptop because the victim is more likely to carry it around […] Over time, as the victim meets associates and friends, the attackers will catalog the various devices encountered, most likely mobile phones. This way the attackers can build a map of interactions with various people—and identify the victim's social and professional circles. By measuring the strength of radio signals broadcast by devices indexed by Flame, attackers in airports, city streets, and other locations might be able to measure the comings and goings of a host of people […] BeetleJuice could be used to upload contacts, text messages, photos, and other data stored on Bluetooth devices, or to bypass firewalls and other security mechanisms when exfiltrating sensitive information" (Goodin 2012).

3. *Right to Development through the Internet*. This right includes the need of poverty reduction and human development (information and communication technologies shall be designed, developed and implemented to contribute to sustainable human development and empowerment), and environmental sustainability (the Internet must be used in a sustainable way, and this relates to the disposal of e-waste and to the use of the Internet for the protection of the environment);
4. *Freedom of Expression and Information on the Internet*. This important issue concerns freedom of online protest (everyone has the right to use the Internet to organize and engage in online and offline protest), freedom from censorship (everyone has the right to use the Internet without censorship in any form, and this includes freedom from any measures designed to intimidate Internet users or close down expression online, including freedom from cyber attacks and freedom from harassment online; freedom from censorship online also includes freedom from blocking and filtering. Blocking and filtering systems which aim to prevent access to content and are not end-user controlled are a form of prior censorship and cannot be justified. Internet intermediaries must never be pressured by states or other parties to remove, hide or block content, or disclose information about Internet users), right to Information (everyone has the right to seek, receive and impart information and ideas through the Internet, and everybody has the right of access to make effective use of government information, which must be released in a timely and accessible manner, according national and international law), freedom of the media (the freedom and pluralism of the media shall be respected), freedom from hate speech (the beliefs and opinions of others must be respected, online as well as offline, and as laid out in Article 20 of the ICCPR, "any advocacy of national, racial or religious hatred that constitutes incitement to discrimination, hostility or violence shall be prohibited by law"). In the document is outlined that certain very specific limitations to the right to freedom of expression may be undertaken on the grounds that they cause serious injury to the human rights of others. However, this must not be used to protect abstract or subjective notions or concepts, or institutions, but rather to protect individuals and groups of people, and restrictions must meet the standards for all restrictions of the right to freedom of expression;
5. *freedom of religion and belief on the Internet*;
6. *freedom of online assembly and association*;
7. *Right to Privacy on the Internet*. This point regards national legislation on privacy (states must establish, implement and enforce comprehensive legal frameworks to protect the privacy and personal data of citizens, and these must be in line with international human rights and consumer protection standards, and must include protection from privacy violations by the state and by private companies), privacy policies and settings (privacy policy and settings of all services must be easy to find, and the management of privacy settings must be comprehensive and optimised for usability), standards of confidentiality and integrity of IT-Systems (the right to privacy must be protected by standards of confidentiality and integrity of IT- Systems, providing protection against others accessing IT-Systems without consent), protection of the virtual personality (everyone has a right to a

virtual personality, and the virtual personality of the human person, i.e. the personal identification in information systems, is inviolable), but the virtual personality of human persons must be respected, however, the right to a virtual personality must not be misused to the detriment of others, right to anonymity and to use encryption (every individual has the right to communicate anonymously on the Internet, and everyone has the right to use encryption technology to ensure secure, private and anonymous communication), freedom from surveillance (everyone has the freedom to communicate without arbitrary surveillance or interception, including behavioural tracking, profiling, and cyber-stalking, or the threat of surveillance or interception).

8. *Right to Digital Data Protection*. As enshrined in Art 12 of the UDHR everyone has the right to privacy. An important aspect of this right is that everyone has the right to protection of personal data concerning him or her. On the Internet, the right to protection of personal data includes protection of Personal data (fair information practices should be enacted into national law to place obligations on companies and governments who collect and process personal data, and give rights to those individuals whose personal data is collected), obligations of data collectors (the collection, use, disclosure and retention of personal data must all meet transparent privacy-protecting standards and everyone has the right to exercise control over the personal data collected about them and its usage. Whoever requires personal data from persons, shall request the individual's informed consent regarding the content, purposes, storage location, duration and mechanisms for access, retrieval and correction of their personal data, and everyone has a right to access, retrieve and delete the personal data collected about them), minimum Standards on Use of Personal Data (when personal information is required, only the minimum data necessary must be collected and for the minimum period of time for which this is required, data must be deleted when it is no longer necessary for the purposes for which it was collected, data collectors have an obligation to seek active consent and to notify people when their information has been forwarded to third parties, abused, lost, or stolen. Appropriate security measures shall be taken for the protection of personal data stored in automated data files against accidental or unauthorised destruction or accidental loss as well as against unauthorised access, alteration or dissemination), monitoring by Independent Data Protection Authorities (data protection should be monitored by independent data protection authorities, which work transparently and without commercial advantage or political influence);
9. *right to Education on and about the Internet*. As enshrined in article 26 of the UDHR, "everyone has the right to education". Everyone has the right to be educated about the Internet and to use the Internet for education, and on the Internet the right to education includes education *through* the Internet (virtual learning environments and other sorts of multimedia, learning and teaching platforms shall take into account local and regional variations in terms of language, pedagogy and knowledge-traditions. Publications, research, text books, course materials and other kinds of learning materials shall be published as Open Educational Resources with the right to freely use, copy, reuse, adapt, translate and redistribute them.

Free or low-cost training opportunities, methodologies and materials related to using the Internet for social development shall be promoted), education *about* the Internet and Human Rights (Everyone shall be educated about the Internet, and education on the Internet shall include raising awareness and respect for human rights, online and offline, and digital literacy shall be a key component of education. Knowledge and skills enable people to use and shape the Internet to meet their needs);

10. *right to Culture and Access to Knowledge on the Internet*. As enshrined in Article 27 of the UDHR, "everyone has the right freely to participate in the cultural life of the community, to enjoy the arts and to share in scientific advancement and its benefits". Also enshrined in Article 27 of the UDHR, "everyone has the right to the protection of the moral and material interests resulting from any scientific, literary or artistic production" of which he or she is author. Intellectual property is a social product and has a social function. Thus, intellectual property protection must balance the rights of creators with the public interest. Copyright regimes must not disproportionately restrict the capacity of the Internet to support public access to knowledge and culture. On the Internet the right to freely participate in culture includes right to participate in the cultural life of the community (everyone has the right to use the Internet to access knowledge, information and research, and everyone has the freedom to access and share information of public value without being subject to harassment or limitations. Everyone has also the right to make use of the knowledge and instruments of the past to enhance the personal and collective knowledge of the future), diversity of languages and cultures (the public service value of the Internet shall be protected, including access to quality and diverse information as well as different cultural content. The Internet shall represent a diversity of cultures and languages in terms of appearance and functionality. Cultural and linguistic diversity on the Internet must be realized in all forms (e.g. text, images and sound). Technological evolution and innovation to promote diversity on the Internet shall be promoted. Indigenous knowledge shall be protected and promoted online), right to use one's own language (all individuals and communities have the right to use their own language to create, disseminate, and share information and knowledge through the Internet. Special attention shall be given to promoting access for minority languages. This includes promotion of the technology and content required to access and use domain names, software, services and content in minority languages and scripts), freedom from Restrictions of Access to Knowledge by Licensing and Copyright (creators have the right to be remunerated and acknowledged for their work and innovations. However, this must be achieved in ways which do not restrict further innovation or access to public and educational knowledge and resources. Licensing and copyright of content must permit knowledge to be created, shared, used and built upon. Permissive licensing models shall be used. Internationally accepted "fair use" exceptions and limitations to copyright must be used, including making copies for personal and classroom use, format conversion, library lending, review, critique, satire, research and sampling. Techniques

which prevent "fair use" exceptions must be prohibited), knowledge Commons and the Public Domain (publicly funded research and intellectual and cultural work must be made available freely to the general public, where possible), free/Open Source Software and Open Standards (open standards and open formats must be made available. Free/libre and Open Source Software (FOSS) must be used, promoted and implemented in public and educational institutions and services. When a free solution or open standards do not exist, the development of the needed software shall be promoted);

11. *Rights of children and the Internet*. Children are entitled to all of the rights in the Charter. Furthermore, as enshrined in Article 25 of the UDHR, childhood is "entitled to special care and assistance". As enshrined in Article 5 of the CRC young people are entitled to respect for their "evolving capacities". In terms of the Internet this means that children must both be given the freedom to use the Internet, and also protected from the dangers associated with the Internet. The balance between these priorities shall depend on the young person's capabilities. The State must respect the rights and responsibilities of parents and the extended family to provide guidance for the child which is appropriate to her or his evolving capacities. On the internet the right to special care and assistance and respect for evolving capacities of children includes right to benefit from the Internet (children should be able to benefit from the Internet according to their age. Children must have opportunities to use the Internet to exercise their civil, political, economic, cultural and social rights. These include rights to health, education, privacy, access to information, freedom of expression and freedom of association), freedom from exploitation and child abuse imagery (children have a right to grow up and develop in a safe environment that is free from sexual or other kinds of exploitation. Steps must therefore be taken to prevent the use of the Internet to violate the rights of children, including through trafficking and child abuse imagery. However, such measures must be narrowly targeted and proportionate. The effect of measures taken on the free flow of information online must be given due consideration), right to have views heard (children who are capable of forming their own views have the right to express them in all Internet policy matters that affect them, and their views shall be given due weight according to their age and maturity), best interests of the Child (as enshrined in Article 3 of the CRC, "in all actions concerning children, whether undertaken by public or private social welfare institutions, courts of law, administrative authorities or legislative bodies, the best interests of the child shall be a primary consideration");
12. *Rights of people with disabilities and the Internet*. People with disabilities are entitled to all of the rights in the Charter. As enshrined in Article 4 of the United Nations Convention on the Rights of Persons with Disabilities (CRPD), "States Parties undertake to ensure and promote the full realisation of all human rights and fundamental freedoms for all persons with disabilities without discrimination of any kind on the basis of disability". The Internet is important in enabling persons with disabilities to fully enjoy all human rights and fundamental freedoms. Special measures must be taken to ensure that the Internet is accessible, available

and affordable. On the Internet, the rights of people with disabilities include Accessibility to the Internet (persons with disabilities have a right to access, on an equal basis with others, to the Internet. Such access must be promoted through: the development, promulgation and monitoring of minimum standards and guidelines for accessibility; the provision of training on accessibility issues facing persons with disabilities; and the promotion of other appropriate forms of assistance to people with disabilities to ensure their access to information), availability and affordability of the Internet (steps must be taken to ensure the availability and effective use of the Internet by people with disabilities. Research and development must be undertaken to promote the availability of Information and Communications Technologies in a format suitable for persons with disabilities. Priority should be given to developing technologies at an affordable cost. Persons with disabilities have the right to accessible information about assistive technologies, as well as other forms of assistance, support, services and facilities);

13. *Right to work and the Internet*. As enshrined in Article 23 of the UDHR: "everyone has the right to work". On the Internet, the right to work includes respect for Workers' Rights (everyone has the right to use the Internet to form trade unions, including the right to promote one's own interests and gather in freely elected organs of representation), Internet at the workplace (workers and employees shall have Internet access at their work place, where available. Any restrictions on Internet use in the work place shall be explicitly stated in staff or organizational policies. The terms and conditions for surveillance of the Internet use of employees must be clearly stated in work place policies and comply with the right to data protection), work on and through the Internet (all people shall have the right to seek employment and to work through or by means of the Internet);
14. *Right to Online Participation in Public Affairs*. As enshrined in Article 21 of the UDHR, "everyone has the right to take part in the government of his [or her] country, directly or through freely chosen representatives". On the Internet the right to take part in the government of one's country includes the right to equal access to electronic services (Article 21 of the UDHR also states that "everyone has the right of equal access to public service in the country". Everyone has the right to equal access to electronic services in his country), the right to participate in electronic government (where electronic government is available, everyone must have the right to participate);
15. *Rights to Consumer Protection on the Internet*. Everyone must respect, protect and fulfill principles of consumer protection on the Internet. E-Commerce must be regulated to ensure that consumers receive the same level of protection as they enjoy in non-electronic transactions;
16. *Right to Health and Social Services on the Internet*. As enshrined in Article 25 of the UDHR, "Everyone has the right to a standard of living adequate for the health and well-being of himself [or herself] and of his [or her] family, and necessary social services, and the right to security in the event of unemployment, sickness, disability, widowhood, old age or other lack of livelihood in circumstances

beyond his [or her] control". On the Internet the right to a standard of living adequate for health includes the access to health-related content online. Everyone shall have access to health-related and social services on the Internet;

17. *Right to Legal Remedy and Fair Trial for actions involving the Internet*. This right includes the right to a legal remedy (as enshrined in Article 8 of the UDHR, "everyone has the right to an effective remedy by the competent national tribunals for acts violating the fundamental rights granted him [or her] by the constitution or by law"), the right to a fair trial (as enshrined in Article 10 of the UDHR, "everyone is entitled in full equality to a fair and public hearing by an independent and impartial tribunal, in the determination of his [or her] rights and obligations and of any criminal charge against him [or her]". Criminal trials must follow fair trial standards as defined by the UDHR (Articles 9–11) and the ICCPR (Articles 9 and 14–16) as well as other pertinent documents. It is increasingly common for the right to a fair trial and to an effective remedy to be violated in the Internet environment, for example with Internet intermediary companies being asked to make judgements about whether content is illegal and encouraged to remove content without a court order. It is therefore necessary to reiterate that procedural rights must be respected, protected and fulfilled on the Internet as they are offline, the right to Due Process (everyone has the right to due process in relation to any legal claims or possible violations of the law regarding the Internet);
18. *right to Appropriate Social and International Order for the Internet*. As enshrined in Article 28 of the UDHR, "Everyone is entitled to a social and international order in which the rights and freedoms set forth in this Declaration can be fully realized". On the Internet the right to an appropriate social and international order includes Governance of the Internet for Human Rights (the Internet and the communications system must be governed in such a way as to ensure that it upholds and expands human rights to the fullest extent possible. Internet governance must be driven by principles of openness, inclusiveness and accountability and exercised in transparent and multilateral manner), multilingualism and Pluralism on the Internet (the Internet as a social and international order shall enshrine principles of multilingualism, pluralism, and heterogeneous forms of cultural life in both form and substance), effective Participation in Internet Governance (everyone has the right to participate in the governance of the Internet. The interests of all those affected by a policy or decision shall be represented in the governance processes, which shall enable all to participate in its development. Full and effective participation of all, in particular disadvantaged groups in global, regional and national decision-making must be ensured);
19. *duties and Responsibilities on the Internet*. As enshrined in Article 29 of the UDHR, "Everyone has duties to the community in which alone the free and full development of his personality is possible". On the Internet the duties of everyone to the community include the respect for the Rights of Others (everybody has the duty and responsibility to respect the rights of all individuals in the

online environment), the responsibility of power holders (power holders must exercise their power responsibly, refrain from violating human rights and respect, protect and fulfill them to the fullest extent possible).

4.7 The "Bill of Rights" Projects

4.7.1 The Internet Bill of Rights Drafted Within the IGF Works

The will to try to develop a set of rules that reflect fundamental principles has spread worldwide in the mid-2000s, leading to the creation of a series of "bill of rights" for the digital world, a list of necessary guarantees aimed at making sure which are the fundamental rights recognised in the digital landscape.[24]

These bill of rights have had different origins: some have been drawn up by activists, other by government bodies – or self-government bodies –, others by states and governments themselves.

Have all, more or less, similar characteristics: the protection of freedom of expression and the extension to the network of principles already established for traditional rights.

The relationship between these bill of rights and the activities of digital resistance which was mentioned above is very controversial. In some ways, they are very generic: the digital dissident is more interested into the margins of freedom and rules of the country in which operate but, on the other hand, these provisions have great cultural value and clear is the will to recognize inviolable rights also in the electronic world (especially in those states where Constitutions do not have similar guarantees).

For the purposes of my study, I will consider very heterogeneous projects: a project of a Internet Bill of Rights drafted within the IGF works, a bill proposed by the Internet Rights and Principles Dynamic Coalition, a proposal coming from a North American scholar and a draft bill of rights for the privacy of the users of social networks drafted by EFF.

First of all, in 2007 a joint statement from Italy and Brazil announced the launch of a new and truly laudable project, championed by the noted Italian academic and scholar Stefano Rodotà,[25] aimed at creating an *Internet Bill of Rights*, a sort of

[24] The idea of a "bill of rights" recalls the *English Bill of Rights* of 1689 (a document declaring, *inter alia*, the rights of citizens and the Parliament against the Crown, especially the rights of petition, of an independent judiciary system, of a control of the taxation system, of free elections of Parliament members, of freedom of speech and freedom from cruelty in punishments and trials and from punishments without trial) and the collective name given to the first ten Amendments to the Constitution of the United States, Amendments that were drafted and came in effect between 1789 and 1791 (protecting, *inter alia*, rights of liberty and property, freedoms of religion, speech, a free press, free assembly, and free association).

[25] See Rodotà 20 November 2007, Una Carta dei diritti del web, Repubblica, http://www.repubblica.it/2007/11/sezioni/scienza_e_tecnologia/rodota-web/rodota-web/rodota-web.html. Accessed 14 November 2011.

"Constitution" for the Internet, containing a list of unalienable rights in the digital era, and, above all, seeking to identify the best methods, on both the national and international levels, to further develop and enforce these rights.

Professor Rodotà explained clearly the purposes of this project:

> […] has jumped in the foreground the importance of a global policy of rights. […] the Internet Bill of Rights is a tool to secure freedom and rights in the largest public space that humanity has ever known. […] can you leave the protection of fundamental rights on the Internet only at the initiative of individuals, which tend to offer only guarantees compatible with their interests and that, in the absence of other initiatives, will appear as the only 'institutions' able to intervene? Can you accept a privatization of Internet governance, or is essential to ensure that a plurality of actors, from many different levels, can communicate and develop common rules, according to a template defined precisely multistakeholder and multilevel? The Internet Bill of Rights, in fact, is not conceived as a transposition in the sphere of the Internet of the traditional logic of international conventions. The choice of the old formula of the Bill of Rights has symbolic highlights that we do not want to limit the freedom network but keep the conditions so that it can continue to flourish, to serve this 'constitutional' guarantees. Let us not forget that Amnesty International has denounced the proliferation of cases of censorship, 'a virus that can change the nature of the Internet, making it unrecognizable' if no appropriate measures will be taken (Rodotà 2007).

Rodotà explains how this movement for a new bill of right must start "bottom-up":

> But, according to the nature of the Internet, the recognition of principles and rights cannot be lowered from above. Must be the result of a process, a broad participation of a variety of subjects that have already materialized in the form of 'dynamic coalitions', groups of different nature, born spontaneously in the network, and in Rio have found a first opportunity for comparison, the joint work of direct influence on decisions. During this process you will be able to attain partial results, the integration between codes of conduct and other forms of discipline, common regulations for individual areas of the world, as again demonstrates the European Union, the region of the world where more intense is the protection of the rights. The traditional objections-who is the legislature? Which court will apply the rights proclaimed? -belong to the past, do not realize that 'the avalanche of human rights is sweeping the last trenches of State sovereignty' […] At the same time as the way the Internet Bill of Rights becomes more already shipped, there will be a change. Will begin to be visible from a different cultural model, born from the realization that the Internet is a world without borders. A model that will encourage the circulation of ideas and will soon be a reference to the 'global community of courts', to the crowd of judges who, in the most different systems now, they face the same issues raised by scientific and technological innovation, giving voice to those fundamental rights which are today the only power opposable to the strength of economic interests. Neither utopia, nor escape forward. Already today, in the aftermath of the Rio Conference, many are at work and are clear directions for the work of the next few months: inventory of 'dynamic coalitions' and creating a platform that allows for dialogue and cooperation; inventory of the many existing documents, to identify what can be the principles and rights at the base of the Internet Bill of Rights (a list is in the Italo-Brazilian); elaboration of a first draft will be discussed in the network. The seeding was good. But the harvest will be equally fervent spirits that will support future actions. (Rodotà 2007).

The initiative eventually stalled, but not before participants were able to define a number of values to be protected on the electronic frontier. Considered especially important were matters related to privacy, the protection of data, the freedom of speech, universal access, network neutrality, platform interoperability, the use of open formats and standards, free access to information and knowledge, the right to innovation and the protection of markets and consumers.

As Kulesza notes about this initiative, the works concerning the Internet Bill of Rights inside the Internet Governance Forum started from the principles of the Universal Declaration of Human Rights and the European Convention on Human Rights, and the freedom of speech, so important in those documents, was the first very common freedom to be limited on the Internet.

The author remarks that the scope is to found a common ground and to try to find an harmonization concerning freedom of speech on the Internet, and it is more from a user point of view.

The idea is not to try to redefine the rights that already exist but rather to build on them and to specify the existing rights in the aspect of their applicability to the Internet environment and to propose new rights and liberties to protect, like net neutrality and interoperability (Kulesza 2008).

4.7.2 The Internet Rights and Principles Dynamic Coalition Bill of Rights

Also the Internet Rights and Principles Dynamic Coalition, an open network of individuals and organisations working to uphold human rights in the Internet environment, drafted a bill with ten key rights and principles that must form the basis of Internet governance.

1. Universality and Equality: all humans are born free and equal in dignity and rights, which must be respected, protected and fulfilled in the online environment.
2. Rights and Social Justice: the Internet is a space for the promotion, protection and fulfilment of human rights and the advancement of social justice. Everyone has the duty to respect the human rights of all others in the online environment.
3. Accessibility: everyone has an equal right to access and use a secure and open Internet.
4. Expression and Association: everyone has the right to seek, receive, and impart information freely on the Internet without censorship or other interference. Everyone also has the right to associate freely through and on the Internet, for social, political, cultural or other purposes.
5. Privacy and Data Protection: everyone has the right to privacy online. This includes freedom from surveillance, the right to use encryption, and the right to online anonymity. Everyone also has the right to data protection, including control over personal data collection, retention, processing, disposal and disclosure.
6. Life, Liberty and Security: the rights to life, liberty, and security must be respected, protected and fulfilled online. These rights must not be infringed upon, or used to infringe other rights, in the online environment.
7. Diversity: cultural and linguistic diversity on the Internet must be promoted, and technical and policy innovation should be encouraged to facilitate plurality of expression.
8. Network Equality: everyone shall have universal and open access to the Internet's content, free from discriminatory prioritisation, filtering or traffic control on commercial, political or other grounds.

9. Standards and Regulation: The Internet's architecture, communication systems, and document and data formats shall be based on open standards that ensure complete interoperability, inclusion and equal opportunity for all.
10. Governance: Human rights and social justice must form the legal and normative foundations upon which the Internet operates and is governed. This shall happen in a transparent and multilateral manner, based on principles of openness, inclusive participation and accountability.

4.7.3 A Bill of Rights in Cyberspace

The North American scholar (and blogger) Jeff Jarvis[26] proposed, last year, an interesting document called "a bill of rights in cyberspace".[27] This "bill of rights" attempts to identify and establish some *fundamental freedoms* of Internet that must be protected against abridgment by governments, companies, institutions, criminals, subverters or mobs.

The first point outlined by the scholar is the *right to connect*, a preamble and precondition to the American First Amendment: before we can speak, Jarvis says, we must be able to connect. Jarvis cites Hillary Clinton's definition of freedom to connect as "the idea that governments should not prevent people from connecting to the internet, to websites, or to each other[28]" and notes that this is the principle that also informs discussion of net neutrality (Jarvis 2010).

The second remark concerns the *right to speak freely*. Jarvis notes that no one may abridge freedom of speech. He acknowledges the limitations on freedom of speech but they must defined as narrowly as possible, and freedom must be the default (Jarvis 2010).

The third right is the *right to speak in our languages*. The author remarks that the English language's domination of the internet has faded as more languages and alphabets have joined the net, which is to be celebrated but also raises the necessity to build bridges across languages. We will want to speak in our own languages, remarks Jarvis, but also speak with others (Jarvis 2010).

The fourth point is the *right to assemble*, that in the American Bill of Rights is listed separately from the right to speak. The internet enables people to organize without organizations and collaborate and that now threatens repressive regimes as much as speech (Jarvis 2010).

The fifth point is the *right to act*, a direct consequence to the right to speak and the right to assemble and the best way to change the world (Jarvis 2010).

---

[26] See http://www.buzzmachine.com/. Accessed 14 November 2011.

[27] See http://www.buzzmachine.com/2010/03/27/a-bill-of-rights-in-cyberspace/. Accessed 14 November 2011.

[28] See Hillary Rodham Clinton's remarks on Internet freedom at the address http://www.state.gov/secretary/rm/2010/01/135519.htm. Accessed 14 November 2011.

The sixth point is the *right to control data*, intended as a full access to our data. Internet, according to Jarvis, must operate on a principle of portability, so information and creations cannot be held prisoner by a service or government and the citizen retains data control (Jarvis 2010).

The seventh point is the *right to own identity*, intended as a right to control the identity online, including names, addresses, speech, creations, actions, connections. In this point is involved also the action of maintaining anonymity in repressive regimes and hiding the identity, or protecting anonymity online to protect the dissenter and the whistleblower (Jarvis 2010).

The eight point is the *attention to public goods* (Jarvis 2011), moving from the premise that Internet is public, is a public place rather than a medium and must not be restricted because what is public is owned by the public and making the public private or secret serves as a means of control (Jarvis 2010).

The ninth point it the *openness of the Internet*, and is related to open-standards use because is the Internet's openness that gives it its freedom and the network must not be controlled by a company or a proprietary standard (Jarvis 2010).

4.7.4 The EFF Bill of Privacy Rights for Social Network Users

In 2010 the EFF drafted a *Bill of Privacy Rights for Social Network Users*, a series of principles to be adopted by social network service suppliers, most particularly *Facebook*. EFF's project identifies three fundamental rights: (1) *the right to informed decision making* (clear user interface allowing informed choices with regard to privacy and security matters), (2) *the right to control* (users must retain full control over the use and disclosure of their data) and (3) *the right to leave* (the user must have the possibility to leave both the platform and the service when he or she wishes, and to fully remove all his or her data).

The first principle deals with the right to informed decision making, and the proposal is clearly divided into three points (EFF 2010):

1. users should have the right to a clear user interface that allows them to make informed choices about who sees their data and how it is used;
2. users should be able to see readily who is entitled to access any particular piece of information about them, including other people, government officials, websites, applications, advertisers and advertising networks and services;
3. whenever possible, a social network service should give users notice when the government or a private party uses legal or administrative processes to seek information about them, so that users have a meaningful opportunity to respond.

This first part of the bill poses several problems. A clear information, first of all, about the data processed and how they are used, but attention, also, to the technical people or the officials who can see the data of the users. An interesting point, for example, could be the case of investigations on Facebook without the user's knowledge.

The second principle included in this bill is about the right to control. It is a very complex and articulated principle, and is divided into seven categories/rights (EFF 2010):

1. social network services must ensure that users retain control over the use and disclosure of their data;
2. a social network service should take only a limited license to use data for the purpose for which it was originally given to the provider;
3. when the service wants to make a secondary use of the data, it must obtain explicit opt-in permission from the user;
4. the right to control includes users' right to decide whether their friends may authorize the service to disclose their personal information to third-party websites and applications;
5. social network services must ask their users' permission before making any change that could share new data about users, share users' data with new categories of people, or use that data in a new way;
6. changes like this should be 'opt-in' by default, not 'opt-out', meaning that users' data is not shared unless a user makes an informed decision to share it;
7. if a social network service is adding some functionality that its users really want, then it should not have to resort to unclear or misleading interfaces to get people to use it.

This second part includes and debates a theme already known to scholars of privacy and data retention, and refers to the awareness or the holder of the data subject about the life of the data itself.

The third part of the bill deals with a sort of *right to leave*. It is very important, and can be divided into three main actions:

1. users giveth, and users should have the right to taketh away. One of the most basic ways that users can protect their privacy is by leaving a social network service that does not sufficiently protect it;
2. a user should have the right to delete data or her entire account from a social network service. And we mean really delete. It is not enough for a service to disable access to data while continuing to store or use it. It should be permanently eliminated from the service's servers;
3. furthermore, if users decide to leave a social network service, they should be able to easily, efficiently and freely take their uploaded information away from that service and move it to a different one in a usable format. This concept, known as 'data portability' or 'data liberation', is fundamental to promote competition and ensure that users truly maintain control over their information, even if they sever their relationship with a particular service.

This last, fundamental aspect concerns the deletion of data and the ability for a user to choose really to leave a service without leaving traces.

4.8 A Human Rights Approach to the Mobile Internet

A Horner's 2011 study concerning how mobile Internet can help to advance human rights and capacities through providing new opportunities for citizens to share information and ideas and to participate in public life, outlined a sort of "human rights approach" to the mobile Internet that is very interesting.

Premises of this particular study are that mobile phones facilitate instant and ubiquitous communication, thereby increasing the power of citizen journalism, crowdsourcing and other forms of expression, and help to bridge the digital divide for people who do not have access to computers and fixed-line connections.

There are, indeed, a number of challenges that need to be addressed in order to harness the full potential of the mobile Internet for universal human rights and citizen empowerment.

The author highlights, for example, high access costs, limitations in the usability of hardware and software for first time users, unequal capacities to create and access relevant content, the closed architecture of the mobile Internet, the persistence of social inequality and lack of respect for cultural diversity.

In this interesting "human rights approach", according to this scholar, the primary goal of regulation and policy should be to fulfil human rights, and there are a number of rights that are affected by the access to the network and the use of different types of communication media.

Freedom of expression is the most obvious of these, including the right to seek, receive and impart information and ideas, but also rights to education, an adequate standard of living, to associate freely with others, to participate in government, to participate in cultural life, and to enjoy the benefits of scientific advancement. Last, but not least, media and technology should therefore be accessible to all, and function in ways that empower citizens to participate in public debate and decision-making, and control their own lives.

The author proposes that policy, regulation and legislation should aim to produce media and communications environments in which four issues are resolved:

1. everyone's human rights must be protected from violation. For example: communications should be free from censorship and surveillance that violates rights to free expression and privacy;
2. everyone's human rights must be positively fulfilled. For example: communications are not only free from censorship, but people also have the capacities that they need to seek different forms of knowledge and express themselves effectively in the public sphere;
3. everyone must be empowered to control their own lives through having meaningful opportunities to access to knowledge, develop their livelihoods, participate in the public sphere, and make their voices heard by political and other leaders;
4. all people must have equal ability to appropriate and innovate with communications media and technologies, adapting them to meet their own needs.

Conclusions are clear: there are three main issue that are in discussion.

1. the evolution and spread of the mobile internet presents exciting new opportunities for the effective implementation of human rights. It can expand people's capacities to create and share information and ideas and is allowing to improve access to the internet for people who cannot afford or do not have physical connections to the fixed-line internet (Horner 2011: 15);

2. it is also making citizen-driven communication more powerful through providing instant and portable connectivity so that people can access and upload information whenever and wherever they need to (Horner 2011: 15);
3. however, the mobile Internet will not necessarily provide a straightforward or unproblematic solution to problems of digital and political exclusion. If we are to foster the evolution of a universally empowering mobile Internet, we will need to address a number of significant challenges relating to affordability, usability, relevant content, network and applications architecture, inequality and identity (Horner 2011: 15).

4.9 The Relationship Between Human Rights and Technology Sales to Oppressive Regimes

In 2012, the *Electronic Frontier Foundation* released a white paper ("Human Rights and Technology Sales: How Corporations Can Avoid Assisting Repressive Regimes") regarding the fact that authoritarian governments around the world are relying on technology produced by American, Canadian, and European companies to facilitate human rights abuses.

EFF, in this study, outlines how corporations can avoid assisting repressive regimes. Briefly, the whitepaper calls on companies to increase transparency around their transactions with potentially repressive regimes and to implement "Know Your Customer" standards for auditing technology sales, including review of the purchasing government's technical questions and customization requests.

If the review indicates that the technologies or transaction may be used to facilitate human rights violations, the company should refrain from participating.

References

Bobbio, Norberto. 1988. Presente e avvenire dei diritti dell'uomo. http://www.giuffre.it/age_files/dir_tutti/strenne/1988/Presente%20e%20avvenire%20dei%20diritti%20dell'uomo%20-%20Norberto%20Bobbio.pdf. Accessed 1 Nov 2011.

EFF. 2010. A bill of privacy rights for social network users. https://www.eff.org/deeplinks/2010/05/bill-privacy-rights-social-network-users. Accessed 14 Nov 2011.

Flear, Mark L., and Anastasia Vakulenko. 2010. A human rights perspective on citizen participation in the EU's governance of new technologies. *Human Rights Law Review* 10(4): 661–688.

Forsythe, David P. 1985. The United Nations and human rights, 1945–1985. *Political Science Quarterly* 100(2): 249–269.

Goodin, D. 2012. Spy software's Bluetooth capability allowed stalking of Iranian victims. http://arstechnica.com/security/2012/06/spy-softwares-bluetooth-capabilty-allowed-stalk-of-iranian-victims/. Accessed 10 June 2012.

Jarvis, Jeff. 2011. A bill of rights in Cyberspace. http://www.buzzmachine.com/2010/03/27/a-bill-of-rights-in-cyberspace/

Horner, Lisa. 2011. A human rights approach to the mobile internet. http://www.apc.org/en/system/files/LisaHorner_MobileInternet-ONLINE.pdf. Accessed 12 Nov 2011.

Kulesza, Joanna. 2008. Freedom of information in the global information society – the question of the Internet Bill of Rights. *University of Warmia and Mazury in Olsztyn Law Review* 1: 81–95.

La Rue, Frank, and Olof Ehrenkrona. 2010. Chairmen's conclusion of expert meeting on human rights and the Internet. http://www.sweden.gov.se/content/1/c6/13/93/96/829645b7.pdf. Accessed 23 Oct 2011.

Rodotà, Stefano. 2007. Una Carta dei diritti del web, Repubblica, http://www.repubblica.it/2007/11/sezioni/scienza_e_tecnologia/rodota-web/rodota-web/rodota-web.html. Accessed 14 Nov 2011.

Sartor, Giovanni. 2010. Human rights and the future of the information society. http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1707724. Accessed 25 Oct 2011.

Sartor, Giovanni, and Mario Viola de Azevedo Cunha. 2010. The Italian Google-Case: Privacy, freedom of speech and responsibility of provider for user-generated contents. http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1604411

Saul, Ben. 2002. Election violence in Sri Lanka: Implementing the right to a free and fair election. *Asia-Pacific Journal on Human Rights and Law* 1: 1–39.

Zuckerman, Ethan, Hal Roberts, Jillian York, Robert Faris, and John Palfrey. 2010. Circumvention tool usage report. http://cyber.law.harvard.edu/sites/cyber.law.harvard.edu/files/2010_Circumvention_tool_usage_report.pdf. Accessed 24 Nov 2011.

Chapter 5
The Use of Liberation Technology

5.1 Technical Resistance Tactics

Using technology to more effectively *oppose* repressive authorities in environments where human rights are limited is, perhaps, the most fascinating aspect of the modern history of hacking.

In addition to isolated and occasional cases, or those that are purely theoretical, there have been, throughout the world, acts of rebellion which have often ended tragically, resulting in the imprisonment or even in the death of the activist. These facts are not always widely known: either they occur in countries of little political or strategic interest for the inhabitants of the rest of the world, or the information, filtered and *sanitized* by local authorities, is limited, or incorrect, or even presented to the public as an entirely different sort of crime, the electronic aspects played down or sometimes completely quashed.

Modern "resistance hacking" endeavors may, for the purposes of our discussion, be divided into two broad categories:

1. the first has *technology* at its center. Some individuals are persecuted because their inventions, or discoveries, may be used to circumvent government-imposed restrictions and are, therefore, deemed dangerous by authorities. I am referring, especially, to creators of software designed to thwart web filtering products (for example, which can be used to hack state firewall systems or to circumvent Internet restrictions present in certain countries) and of anonymous web browsing systems, such as *Tor*, now widely used, by hackers and "average web users" alike. Within this first category, hackers operate in a quite linear fashion, first *analyzing* local filtering systems (generally these are either manually controlled by individuals, veritable "censorship armies", who monitor the content of closely followed connections, or implemented through the use of automatic filter or firewall software technologies) and then seeking to "unlock" these systems either from inside their home countries, or, working from outside nations in which they have sought refuge and in which they can operate in a more serene environment,

G. Ziccardi, *Resistance, Liberation Technology and Human Rights in the Digital Age*, Law, Governance and Technology Series 7,
DOI 10.1007/978-94-007-5276-4_5, © Springer Netherlands 2013

offering to assist any other dissidents still remaining behind government firewalls state-mandated filters and other restrictions. Hacking activities in this first category may involve reaching foreign sites containing "unapproved" information, often quite different from that circulated locally by the government-controlled press agencies (and are thus motivated by the desire and need for information that is objective and unadulterated); on the other hand, however, hackers may also be spurred to action by the in a certain sense opposite need to circumvent government restrictions and firewalls in order to inform the world of situations and events occurring within the borders of the country (by posting news to forums, updating blogs, using *Facebook* and *Twitter*). Additionally, hacking may arise from the need to evade monitoring by government organs and committees seeking to control content, from the need to obtain and install software banned in the activist's country of residence (such as VoIP, general encryption software or anonymous web browsers) and even simply from the need to open e-mail boxes managed by foreign providers able to guarantee confidentiality and transparency in their dealings with authorities in the event of seizure of correspondence or monitoring of messages. This first category almost always involves individuals who are hackers in the strictest sense of the word, possessing good computer skills, able to quickly analyze systems and to then use reverse engineering for electronic resistance activities;

2. the second category of modern "protest hacking" slightly overlaps with the first, in one important aspect which, in my opinion, must get special consideration: it is, in fact, centered on *human beings*, on the *individuals* themselves. Here, reference is clearly made to specific individuals, who are generally not, in these cases, hackers in the strict sense of the term, but who, nonetheless, may be incarcerated, intimidated, or denounced because, through the adroit use of available technologies, they have dared to communicate to the world events occurring within their countries. These dissidents almost always work from within the confines of their own countries of residence, albeit with great caution. They use blogs, *Twitter*, *Facebook* to forums to voice their political ideas, and are often accused of offenses that are not strictly connected to the world of technology, but more often related to restrictions on transmitting news or to criticism of authorities. In this framework, then, technology, which cannot be of any concrete assistance once the individual has been definitively identified, can, on the other hand, play an enormously important role in revealing unpleasant information which, so often, authorities throughout the world would rather remained hidden and out of sight.

Which brings us to another fundamental aspect: with the arrival of rapidly multiplying news stories describing the widespread and ever-increasing use of new communication technologies and platforms in repressive countries, *Twitter* and *Facebook* have garnered increased attention and importance. Much has been said of Iran's "Cyber-Revolution" in 2009, with a number of politicians declaring that if not for *Twitter* the protest may never have been possible, leading to wide-spread discussion of how technologies alone might spur revolution. However, it should be noted that, in the end, scholarly thought on the matter has sided against this interpretation,

noting that, in reality, very few tweets had originated from inside Iranian territory during the uprising there (most in fact had been written by individuals in the United States, Turkey, and Switzerland) and that the true means of communication in Iran, during the rebellion, in order to explain to the world what was occurring, had been simple word of mouth. The truth, as I already said, probably lies somewhere in between: *Twitter*, *Facebook* and other instruments are important in protest, or revolutionary, activities, today as never before. They are important as were other communication and broadcasting instruments in diverse historical periods, and can, without the shadow of a doubt, do an enormous amount to facilitate actions and the free flow of information in hostile environments prone to censorship. I feel however, that it is, however, somewhat exaggerated to speak of "Twitter Revolutions" or of uprisings caused and brought to fruition solely as a result of available technologies. There are so many other factors, especially those grounded in the territory and in the human beings inhabiting it, that are considerably more decisive in guaranteeing the success or failure of actions of protest and civil disobedience. Technologies today can certainly be a facilitating factor in revolution, but only when guided by the hearts, brains, and concrete actions of the activists who put them to use.

The first and perhaps still the most widely-known episode of large scale hacking resistance against authorities, extensively followed by the worldwide press at the time, took place in China[1] and involved the so-called *Great Firewall of China*.[2]

[1] See Sect. 6.2.7.

[2] Concerning the interesting (technical) issue of how to circumvent the *Great Firewall of China* (from an introductory point of view), see Copeland notes and his dialogue with a dissident (Copeland 2012): "When I saw Leah (last name withheld until she's back in the U.S.) in May a week before she left for a 3-month trip to China, she admitted it would be difficult to break her Facebook and Twitter habit. But, like any good addict, it took Leah less than a week to get settled and circumvent the Great Firewall of China. Along the way, she learned it was a relatively easy process. Leah, a 21-year-old student at the college where I teach, emailed me this week. She figured out that for about $9, she can download a virtual private network, which effectively nullifies China's efforts to block access to certain websites. Every time she logs onto the Internet, she also signs into the VPN, which gives her access to Facebook, Twitter and all the other sites the Chinese government tries to censor. "It was fairly easy for me to set up," Leah said. China did try to crack down on VPNs last year, but the effort seemed to primarily focus on university and corporate connections. Home users were largely unaffected. China, of course, is not trying to block all users from accessing those sites. An all-encompassing censorship strategy for all of the country's 513.1 million Internet users is not feasible or practical. The government's hope is that if it can make access to Facebook, Twitter and other sites enough of a pain, it will deter most people from bothering […] Six years after Google launched a government-monitored version of its search engine in China, and 2 years after Google said it would stop self-censoring in the country, Leah said few people still use it. They instead opt for the more widely popular Baidu. "Most people wouldn't even think to use Google for online searches the way I would," she said. "I actually had an experience like this the other day when I was asked how I found some information, and I said in an obvious tone that I Googled it, not remembering that normally they wouldn't even think to use Google as a search engine. Leah also noted that Weibo, a Chinese social network that combines Twitter- and Facebook-like features, remains hugely popular as an alternative to the better-known but banned American social networks. And QQ is also gaining traction as an instant messenger, video chat and file-sharing client". (Copeland 2012).

The Chinese framework is typical: similarly to other repressive nations, Chinese authorities implemented a technical filtering system bolstered by strict legislation, to control and monitor the use of Internet within its borders. This global surveillance project was given the name of *The Golden Shield Project* and was promoted by the government's Ministry of Public Security in order to incentivize the adoption of advanced computer and communication technologies capable of reinforcing the police's monitoring and filtering capacities, reactivity times and crime prevention initiatives. The immediate consequence was the creation of an unprecedented network that not only watches, listens in on and records the activities of China's citizens, but at the same time also coordinates an enormous flow of information. Internet monitoring and censorship in China is managed by the *Great Firewall of China*, mentioned above, which operates on myriad levels. The third element in China's censorship regime is the extensive filtering of any foreign web site containing content considered by the authorities to contain ideas contrary to the country's government, or deemed in any way unsuitable for the Chinese population or for the morality of the country. This highly effective triptych (global surveillance + firewall + filtering) has given rise to what is, in all likelihood, the most articulated system to limit the freedom of speech on Internet currently existing.

From a technological point of view, censorship in China is implemented with router level filters throughout the country's internal network and with thorough and widespread monitoring not only of certain IP addresses of specific foreign web sites, including sites hosting blogs, but also of those containing certain blacklisted keywords. In some cases, an even more advanced technique is used, that of *substituting* web pages: when authorities intercept a connection to a site considered to be in any way *inappropriate* or *unsuitable*, the user is automatically redirected to a different site containing government-selected content. As mentioned above, however, more than just technology is used to create a generally inhibitory environment; in addition its extensive technical arsenal, the *Golden Shield Project* may also draw upon an extremely rigid legal framework, which since 1997 has punished anybody seeking to utilize Internet for the purposes of inciting the overthrow of the government or the socialist system, of fomenting division within the country, of transmitting untruths or of presenting misleading information. In the same way, the law establishes that businesses and individuals engaged in Internet activities must accept both supervision and inspection by public security authorities. Thus the discretionary powers of government censorship activities (which are, to say the least, considerable) rest on this powerful combination of vague and imprecise norms and utter dependence of ISPs and ICPs on the whims of government authorities.

China and its censoring activities became the subject of international press coverage in October 2010 when the *Nobel Peace Prize* was awarded to a leading Chinese dissident, Liu Xiaobo, a 54 year-old university literature professor who was serving an 11-year sentence in a prison in the North East of China for "inciting subversion to government power". The event had a number of interesting technological ramifications: in an effort to prevent the news from being circulated and from reaching the jailed dissident (even his wife was placed under house arrest), Chinese authorities created an enormous *block* of the news over all information channels, which continued for many days.

Alongside the critical situation in China, there are cases throughout the world, perhaps somewhat less systematic and pervasive, but nonetheless just as important, all of which contribute to create a global panorama of, on the one had, firm opposition to repressive regimes, and, on the other, reaction by governments and authorities which, in many cases, is not only just as firm but violent as well.

In a quite different political sphere, for example, in Russia,[3] on 16 July 2010, the civil court of Komsomolsk-on-Amur obliged, for the first time ever in that country, a large local provider, *Rosnet*, to block the IP addresses of five web sites accused of not having removed extremist content. A number of worrisome declarations by the public ministry following the case referred to *obligations on the part of providers to filter content*.

Yemen and Iran,[4] on the other hand, have for some time been the two countries in which electronic resistance activity has lead to the concrete development of specially-designed software programs created precisely in order to allow users to oppose the imposition of government technological filtering measures. *Alkasir*,[5] a software program written by the Yemeni programmer Walid Al-Saqaf, allows its users to circumvent blocks and to visualize content on banned or otherwise blocked sites. The site's slogan ("For Mapping and Circumventing Cyber-Censorship") is fairly indicative of the program's functions, operating in close connection with its web site and with proxy servers in order to allow users both to circumvent blocks of specific URLs and, at the same time, to track censoring activities in order to periodically verify whether certain URLs remain blocked, in addition to keeping track of web censorship trends and tendencies generally.

Another widely-known case involved a blog created by a woman from Shanghai, known on the web by her pseudonym *Xiaomi*. Seeking to circumvent censorship systems, she coordinates a group of volunteer translators who use a shared *Google Docs* account and translate texts forbidden by the Chinese government. She then publishes them in her blog and on a public *Google Docs* page.

Court cases involving bloggers, who have been arrested or convicted are frequent, especially in Iran and in China. Famous examples are the Iranian Shiva Nazar Ahari, the Moroccan blogger Bashir Hazzam, and the Vietnamese poet Pham Van Troi, sentenced by the court of Hanoi to 4 years of prison for having diffused his ideas on the Internet. Recently, in Iran, one of the country's most famous bloggers, Hossein Derakhshan, known as the "Blog Father", was sentenced to 19 years in prison for collaborating with the United States, diffusing propaganda against the Islamic system, abetting counter-revolutionary cells and insulting a religious leader.

A young Icelandic legislator, Birgitta Jonsdottir, announced in 2010 that she was planning to present a bill to create in her country a sort of "safe haven" for free speech. The project is called the *Icelandic Modern Media Initiative*, and seeks not only to create a global "free port" for investigative journalism but also to introduce a new set of laws offering journalists and editors the safest and the most powerful

[3] See Sect. 6.2.14.

[4] See Sect. 6.2.6.

[5] See the web page of the project at https://alkasir.com/.

online venue in which to work in full freedom and transparency.[6] The project offers protection for sources and seeks to provide meaningful limitations to the liability of providers hosting news items, and aim to attract not only news creators but also journalists, dissident groups, informative data centers and anybody desiring to be involved in a free information project.

The idea of seeking "areas of world" in which to host a sort of "data paradise" is not exactly new. Several years ago, the tiny *Principality of Sealand*, located 10 km off the coast of Great Britain on a former WWII sea fort in the North Sea, leaped to the front pages of newspapers around the world. Paddy Roy Bates, a pirate radio broadcaster occupied the structure in 1967, declaring it to be an autonomous micro-nation (although, in reality, that *status* has never been recognized by any nation in the world or by any international organization). The wave-swept principality received international publicity when it established a new entity called the *HavenCo*[7] data haven, offering protection to web sites hosting sensitive content and illustrating on numerous occasions how the "extraterritoriality" of its data center could be key to offering safe, unmonitored Internet, and ideal for guaranteeing levels of independence without precedent to its users. There was even an Italian attempt, in the heady year of 1968, to create, just off the coast of Ravenna in the Adriatic sea, another micro-nation, the short-lived *Island of Roses*, which had as "territory" a man-made platform in the Adriatic Sea; the Italian government made short of work of the idealistic project, however, unceremoniously exploding and sinking it (with no loss of life).

An interesting technical project is *The (Amnesic) Incognito Live System*,[8] a live cd or USB key that helps its users protect their privacy and web anonymity by forcing all outgoing connections to go through *Tor*, leaving no trace on local storage unless explicitly requested to do so. Based on *Debian*, the system is designed to aid users in achieving anonymous communication from any venue, using all typical applications, thus not only web browsers but also chat and instant messaging platforms, electronic imaging, office and e-mail programs, are all pre-configured in order to guarantee the highest levels of protection, including shelter from web traffic analysis, without ever leaving a trace. The creators of this system warn that absolute anonymity is nearly impossible to establish (an attacker with sufficient resources can nearly always identify a browser), and that that their objective is simply that of rendering more complex the task of identifying web users, thereby increasing the resources and investments necessary to do so, hopefully to levels that render the browsing activities of the dissident using the software extremely difficult to trace, if not completely secure. This objective is achieved by sending all outgoing traffic through the *Tor* network, rendering it very difficult to track. Furthermore, were someone to attempt to identify the user, the search activities would necessarily come to a stop at the IP address of one of the *Tor* project participants, and not at the protected IP. Finally, anyone attempting to identify the destination would be repeatedly sent back to the very same point.

---

[6] See Sect. 6.2.12.

[7] For a complete overview see the Grimmelmann's study regarding this strange start-up (Grimmelmann 2012).

[8] See the web site of the project at the address http://tails.boum.org/. Accessed 24 November 2011.

5.2 Surveillance Self-Defense or Self-Defense Against Surveillance and Monitoring

In 2009 EFF, the Electronic Frontier Foundation, published a documents and started a project entitled, significantly, *Surveillance Self-Defense*,[9] which sought to provide a guide to using the Internet for political activists in repressive regimes, with particular attention to the situations in Iran and China, but containing a great deal information useful for anybody seeking to protect not only their own rights to free speech rights on the web, but even those of others.

The project has two declared objectives: to communicate the enormous power of Internet as a means of organizing political protest and activism and of communicating events occurring in even the furthest corners of the earth to the entire world, and at the same time to increase awareness of the fact that governments worldwide can and do use internet and the most modern technologies available to monitor, menace and take aim at activists and even at average citizens as well.

This signifies, essentially, that Internet users must always take steps to utilize this tool securely, almost as though we had a video-camera focused on our keyboards, or an open window at our backs.

EFF's concise yet highly instructive guide offers a number of simple suggestions, set out in a well-organized fashion and presented logically and clearly. The article opens, for example, with the far-from banal concept of *risk assessment*: the very first step in defense from digital surveillance is to understand the concept of risk assessment, or, as EFF neatly defines it, the process of deciding which threats are faced, how likely and serious they are, and how to prioritize the steps to be taken in order to protect oneself.

The second step is to pay close attention to (and to be extremely wary of) possible *malware*, that is to say computer viruses, worms, trojan horses, keystroke loggers, rootkits, and any other sort of software that allows a computer to monitor the user's activities or to act against his or her interests. Moreover, if malware has been installed due to a *government initiative*, then it is safe to presume that all files and communications will be subject to surveillance. Thus there are two essential tactics here: either possessing a secure computer of one's own or using extreme caution when using "institutional" or shared computers (for example those found in libraries or Internet cafés). In the second case, users should be aware of and use bootable USB devices or CDs (such as *Incognito*) to mitigate the risks posed by malware.

The third suggestion is to always seek out the least dangerous communication channels available when contacting other individuals and activists. Speaking in person is nearly always the safest way to communicate, unless others are watching or the location is being monitored. Activists should be aware of the risks associated with telephone calls: it is important to remember that phone lines may be monitored. SMS text messages should be avoided, as they are generally unencrypted and may be intercepted and analyzed on a massive scale. It is also essential to encrypt Internet

[9] See the web site of the project at the address https://ssd.eff.org/. Accessed 24 November 2011.

communications and to select trustworthy service providers who are unlikely to cooperate too readily (and without guarantees) with authorities.

The fourth suggestion is too use *encryption tools*. The well-protected user will utilize the most advanced encryption techniques available in order to prevent surveillance. *Tor* is the most recommended. It encrypts communications and "bounces" them about the planet before sending them on to their destination. It offers a high level of protection against surveillance and is fairly user friendly. The greatest difficulty when using *Tor* is that it can slow browsing considerably. The article notes, however, that in some countries simply using *Tor* may lead to increased surveillance, arrest, or worse, and in these cases users are advised to use *Tor* only in combination with a *Tor Bridge*. Further options are the use of an encrypted proxy or a *Virtual Private Network* in order to create a sort of tunnel to route traffic overseas. Also useful, but to be used with care as they tend to be centralized, are services such as *Hotspot Shield*. EFF has contributed to the development of a Firefox extension called *HTTPS Everywhere* which seeks to change the connection from http to https whenever it is possible to do so. It was not designed to substitute *Tor* or VPN but simply provides added protection.

The next step for avoiding surveillance is to use extreme caution regarding the online publishing of *sensitive materials*, especially what is published, and where: activists seeking to elude surveillance should avoid publishing sensitive materials under their own names, or including facts that might reveal their true identities, unless they are willing to take the risks of identification, and possible retaliation, by authorities. It is additionally advisable not to publish material through hosting services that have a commercial presence in the country in which the dissident resides, or which are likely to cooperate with the government. Some nations have treaties with others nations, so it is important to consider the possibility of international cooperation in the enforcement of repressive laws. Strictly in terms of computer security, it would be prudent, whenever possible, to publish only through services using https throughout their sites.

Finally, the sixth and final suggestion, for those who are lucky enough not to live under a repressive regime, is that there are a number of concrete manners in which to *aid* individuals who do need to avoid surveillance. Those interested may activate and run a *Tor Relay*, donating a certain amount of bandwidth to help with the relay of encrypted traffic. Two other possibilities are to run a *Tor Bridge*, or even to run a *Tor* exit node, the machine which passes traffic out of the *Tor* network and on to its final destination on the internet (although it should be noted that this option requires considerable organization and commitment). Additional ways to assist range from running a proxy for individuals in countries where censorship is common to providing them with shell accounts to use to create a personal proxy.

In my opinion, it is useful to bear in mind that, even our globally monitored society, defense against monitoring should generally occur at essentially three main levels. The first is the computer we use and the data it contains. Thus we need to consider possible seizure, searches and theft of both computers and all data storage devices. The second level is comprised of the cables and fibers through which any data we send through the internet will flow, and which may be intercepted and monitored at

any point between the starting and end points. The third level is data that is neither memorized in our computers or pen drives, nor in transit, but already memorized on external services, be they sophisticated and encrypted cloud computing services or commercial and blogging sites or ISP platforms. Protection must occur at all three of these levels, and therefore must be quite varied and at times, if it is to be effective, may need to be extremely complex: from a good data retention and destruction policy to storing (and transmitting) as little information as possible, from effective document and email archive management practices to being careful to delete internet browser chronologies so as not to leave any trace on the computer as to our browsing history, careful attention to our own habits in the digital world can decrease all our chances of being monitored as we go about are daily lives.

5.3 A Recent Circumvention Tool Usage Report

In 2010 Roberts, Zuckerman, York, Faris and Palfrey wrote a report about the usage of circumvention tools around the world. Premises, according to the authors, are clear: circumvention tools allow users to bypass Internet filtering to access content otherwise blocked by governments, workplaces, schools, or even the blocked sites themselves, and there are a number of different types of these tools. The scholars outlines blocking-resistant tools, simple web proxies, virtual private network (VPN) services, and open HTTP/SOCKS proxies, but every type of circumvention tool provides the same basic functionality: proxying user connections to provide access to otherwise blocked sites.

The report explains (Roberts et al. 2010) a variety of methods the scholars tested to evaluate the usage of these tools, also with a critical approach (e.g., they remark that much of the media attention on circumvention tools has been given to a handful of tools, notably *Freegate*, *Ultrasurf*, *Tor*, and *Hotspot Shield*, but they found that these tools represent only a small portion of overall circumvention usage and that the attention paid to these tools has been disproportionate to their usage, especially when compared to the more widely used simple web proxies). Conclusion is that overall usage of circumvention tools is still very small in proportion to the number of Internet users in countries with substantial national Internet filtering.

The scholars remarks three key findings of their study (Roberts et al. 2010):

1. no more than 3% of Internet users in countries engage in substantial filtering use circumvention tools. The actual number is likely considerably less.
2. Many more users use simple web proxies than use either blocking-resistant tools or VPN services. Of the 11 tools with at least 250,000 unique monthly users, 3 are blocking- resistant tools, 1 is a VPN service, and 7 are simple web proxies.
3. When users search for proxy and circumvention related terms in filtering countries, they overwhelmingly search for generic proxy terms like “proxy,” and those terms overwhelmingly return either simple web proxies or sites that list simple web proxies and HTTP/SOCKS proxies, not more sophisticated tools (p. 1).

In this study is outlined that network filtering of the Internet by national governments is documented in over 40 countries worldwide.

Countries use this network filtering as one of many methods to control the flow of online content that is objectionable to the filtering governments for social, political, and security reasons.

Filtering is particularly appealing to governments as it allows them to control content not published within their national borders.

In addition to national Internet filtering by governments, many schools and businesses filter their local connections to the Internet. Many web sites even filter their own content by the geographic location their users – for example, television streaming site hulu.com blocks all users outside of the U.S. from accessing its content.

All circumvention tools use the same basic method to bypass this sort of network filtering: they proxy connections through third party sites that are not filtered themselves.

By using this method, a user in China who cannot reach http://falundafa.org directly can instead access a proxy machine like http://superproxy.com/, which can fetch http://falundafa.org for the user.

The network filter only sees a connection to the proxy machine (superproxy.com), and so as long as the proxy itself remains unfiltered, the user can visit sites through the proxy that are otherwise blocked by the network filter.

Some, but not all, tools also encrypt traffic between the user and proxy, both so that the traffic between the user and proxy is much more difficult to monitor and so, that filtering triggered by the content of the traffic (instead of merely the destination of the traffic) will not work.

Despite this core similarity, circumvention tools differ significantly in many implementation details.

The authors break circumvention tools into four large categories based on their proxy implementations. Each category of tool is distinguished from one another also by virtue of each being closely associated with a single model of financial support.

The four categories of tools are: blocking-resistant tools, simple web proxies, VPN services and HTTP/SOCKS proxies.

The defining characteristic of blocking-resistant tools is that they implement sophisticated methods for evading blocking by filters.

A core problem for all circumvention tools is that proxy sites can be blocked just as content and other sites. China can block superproxy.com as well as falundafa.org, and then proxy requests through superproxy.com will cease working.

Some tools in each of the above categories use simple forms of blocking resistance to avoid this sort of filtering – for example, a simple web proxy might maintain a list of alternative domain names to send to users in the case that one or more of its existing domain names is blocked.

The tools the scholars classify as blocking-resistant tools distinguish themselves from the other categories of tools by implementing much more sophisticated technical means of blocking resistance.

Conclusions are that usage estimates for blocking-resistant tools and for simple web proxies suggest that simple web proxies are at least as popular as the

blocking-resistant tools and are likely an order of magnitude more popular, in aggregate. Of the 11 circumvention tools with at least 250,000 monthly users (Ultrasurf, Freegate, Tor, Hotspot Shield, and SWP #s 1–7), 7 are simple web proxies. Those 7 proxies together appear to serve close to half of the combined unique users of the 183 simple web proxies whose usage we were able to estimate.

The number of subscription-based VPN services has more than tripled over the past 3 years, but the usage of these services, other than Hotspot Shield, is still a relatively small portion of circumvention tool users, totaling about as many users as the largest single blocking-resistant tool or simple web proxy.

This result should not be interpreted to diminish the importance of blocking-resistant tools or VPN services. Tor provides an important anonymizing service as well as enabling circumvention of filtering, and Freegate, Ultrasurf and VPN systems allow users in nations that aggressively filter the Internet to obtain relatively uninterrupted connections to the Internet. VPN services provide significantly more functionality than simple web proxies because they proxy the entire network connection. But this result does suggest that scholars, advocates, and others need to take seriously the role simple web proxies play in enabling circumvention of Internet filtering (Roberts et al. 2010).

5.4 Tools and Guides

5.4.1 Leaping Over the Firewall: A Review of Censorship Circumvention Tools by Freedom House

5.4.1.1 Preliminary Issues Described in the Report

A very detailed document by the scholars Cormac Callanan (Ireland), Hein Dries-Ziekenheiner (Netherlands), Alberto Escudero-Pascual (Sweden) and Robert Guerra (Canada), drafted in 2010, is based on the remark that censorship, on the Internet, poses a growing challenge to freedom of expression online worldwide. Several countries, in fact, filter online content to restrict the ability of citizens to access information; due to these limitations, several tools to *circumvent* censorship are critical for bypass, access and share information.

This study aims to help users to choose the tool that is the most suitable to them if they are going to operate in an environment where the Internet is limited; the second part of the study tries to illustrate differences between each instrument (also testing them Azertbaijan, Burma, China and Iran).

These circumvention tools, the authors explain, are primarily designed to circumvent Internet filtering; that's why the main issue to resolve behind these technologies is to search for *alternative routes* for packets of data, and these alternative routes use one or more collaborative server in order to bypass the locking mechanism of the network.

The report finds that there are four main target (blocking systems) to take into consideration:

1. blocking systems with a service-based approach, like e-mail, web, p2p;
2. blocking systems with a content-based approach, like the block of hate-speech, child pornography, gambling websites, political opposition sites, human rights organizations, independent news sites;
3. blocking systems regarding user-based activities, for example blocking users who download illegal music, who send spam or, in repressive countries, who advocate for human rights;
4. blocking systems with a search engine-based approach, for example preventing search results linked to specific web sites.

The three main technologies that, in the last 10 years, became the most successfully used by digital dissidents all over the world are proxies, tunnelling and onion routing.

Proxies, first of all, are very useful to circumvent Internet blocking that prevents direct access to a foreign based web site: a user can, in fact, ask to a foreign proxy to access the blocked content on his or her behalf. As long as that foreign proxy itself is not being blocked, the authors note, the user can then gain access to the content to bypass local filtering. A disadvantage of proxies is that the application that the Internet user wishes to use (such as a browser or e-mail program) must be "proxy aware", it should have the option to set a proxy as an intermediary access server. This approach also requires that the channel to the proxy not be blocked itself. To make interception of the information harder, all tools that the scholar tested also encrypted the traffic to the proxy: for a regular proxy this is not standard practise, but is generally supported by proxy protocols.

The second technology, tunnelling software, allows users to create an encrypted "tunnel" to a different machine on the Internet that prevents the filtering software from seeing web requests. Once a tunnel is created to the other machine, all internet requests are passed through the tunnel, to the machine on the other side, and then to the internet. The access method is similar to the use of a proxy, except that a tunnel is recognized by the operating system as a separate internet connection: this means that it is possible to use tunnels without a specific setting in the application. VPN tunnels are invariably encrypted and thus not susceptible to snooping (interception of traffic).

The last one, onion routing, uses advanced public key encryption to send encrypted traffic with pre-shared public keys of servers (often called onion routers or mixers) and transmitted to them. It is decrypted once received (often through several stages, passing several routers or mixers along the way) until it reaches the final (exit) node on the network. From that point on, plain, decrypted traffic to the open Internet is provided. Using this principle, makes it possible to employ layered cryptographic safeguards on tunnelled traffic (hence the reference to an onion or a telescope: every cryptographic layer needs to be peeled off before plain text traffic is visible at the exit-node).

5.4.1.2 Typical Circumvention Tools

The are several circumvention tools that are used all over the world; some have been used for a long time, others are recent, or are in constant evolution. It could be very useful, at this state of the study, to list several software packages commonly used by digital dissidents in critical contexts:

1. *DynaWeb*.[10] This interesting tool is, essentially, a web-based anti-censorship portal: users point their web browser at one of the DynaWeb URLs, and a web page will be presented with most blocked web sites as links. In addition, a user can type in any URL in the box on the page and *DynaWeb* will fetch the pages for him/her instantly. Particularity of this product is that no software is needed, nor are any settings tweaked on a user's computer. The site informs that Chinese net police watch *DynaWeb*'s portal web sites closely, and block them as soon as they identify them, so *DynaWeb* must be very dynamic: it has hundreds of mirror sites at anytime, and each with a varying IP and DNS domain name, to defeat IP blocking and DNS hijacking;
2. *Freegate*.[11] This software works by tapping into an anti-censorship backbone (DynaWeb, DIT's P2P-like proxy network system) and its anti-censorship capability is further enhanced by a new, unique encryption and compression algorithm;
3. *Gtunnel*.[12] This software is a *Windows* application that works as a local HTTP or SOCKS proxy server (after setting proxy to *GTunnel* in web browser or other Internet applications, the traffic will go through *GTunnel* and their server farm before it reaches its original destination). This path of the traffic protects Internet users' privacy and freedom of speech because user's IP address is hidden and user's Internet privacy protected. The destination servers see *GTunnel* server addresses instead, traffic content is encrypted with industry-strength algorithms between the user's personal computer and *GTunnel* servers so the local filtering/censorship systems will not see the content in clear-text format;
4. *Google Services*. Several *Google* services can be used (and *are* used) as circumvention tools. Google Translate, for example, can be useful to gather blocked content setting the source language to something different from what it is, and setting the target language to the actual source language. In this case, Google Translate will gather the requested data and leave it non-translated. Also *Google Cache* can be useful for a dissident to access Googles cache servers to gather blocked content. Google Reader, finally, can be used to subscribe to news feeds, which gathers data on the user behalf (it acts like a proxy), and lets the user read it through the *Gmail* web interface;

[10] See the web page of this tool at the address http://www.dit-inc.us/dynaweb. Accessed 27 November 2011.

[11] See the web page of the project at the address http://www.internetfreedom.org/FreeGate. Accessed 24 November 2011.

[12] See the web page of the project at the address http://www.internetfreedom.org/Gtunnel. Accessed 24 November 2011.

5. *HotSpot Shield*.[13] This product protects the identity of the user by ensuring that all web transactions are secured through HTTPS, and makes the identity invisible to third party web sites and ISP's creating a virtual private network (VPN) between the computer and the Internet gateway;
6. JAP.[14] This service uses a single static address which is shared by many JAP users, and in that way neither the visited website, nor an eavesdropper, can determine which user visited which web site. Instead of connecting directly to a webserver, JAP users take a detour, connecting with encryption through several intermediaries, so-called *Mixes*. JAP uses a predetermined sequence for the mixes, and such a sequence of linked mixes is called a *Mix Cascade*. Users can choose between different mix cascades, and since *many users* use these intermediaries at the same time, the Internet connection of any one single user is *hidden* among the connections of all the other users. No one, not anyone from outside, not any of the other users, not even the provider of the intermediary service can determine which connection belongs to which user. The intermediaries (mix providers) are generally provided by independent institutions which officially declare that they do not keep connection log files or exchange such data with other mix providers. JAP shows the identity and number of organisations in each Mix cascade in detail, and verifies this information by cryptographic means. The users are thus able to selectively choose trustable mix cascades;
7. *Psiphon*.[15] This product was developed for the delivering of multimedia Internet content in environments where that content is *filtered* or *blocked*. The initial idea was of a lightweight and easy-to-install (and operate) proxy capable of allowing non-technical users to operate a *private proxy platform* designed to overcome filters on Internet content. *Psiphon* traffic is encrypted to avoid blocking, and this obfuscates the real address of the content someone is trying to access. The software is not designed to be used as anonymity software, and does not provide protection from traffic analysis as a way of determining patterns of online behavior, but is designed to provide a channel to access content which is normally filtered. In other words, it is not a replacement for secure communication environment, won't secure user's e-mail, won't encrypt the user's hard drive, or provide the user with end-to-end anonymity;
8. *Tor*.[16] Tor is probably the most used tool in critical contexts. It was originally designed, implemented, and deployed as a third-generation onion routing project of the U.S. Naval Research Laboratory, with the primary purpose of protecting government communications. Tor is a network of virtual tunnels (Dingledine et al. 2004) that allows people and groups to improve their privacy and security on the Internet. Tor protects against a common form of Internet

[13] See the web site at the address http://hotspotshield.com/. Accessed 24 November 2011.

[14] See the web site at the address http://anon.inf.tu-dresden.de/index_en.html. Accessed 24 November 2011.

[15] See the web site at the address http://psiphon.ca/. Accessed 24 November 2011.

[16] See the *Tor* web site at the address https://www.torproject.org/.

surveillance known as *traffic analysis*, that can be used to infer who is talking to whom over a public network. Knowing the source and destination of Internet traffic allows others to track user's behavior and interests, and Tor was developed to help to reduce the risks of both simple and sophisticated traffic analysis by distributing transactions over several places on the Internet, so no single point can link the user to his/her destination. Instead of taking a *direct route* from source to destination, is explained on Tor web site, data packets on the Tor network take a random pathway through several relays that cover user's tracks, so no observer at any single point can tell where the data came from or where it's going. To create a private network pathway with Tor, the user's software or client incrementally builds a circuit of encrypted connections through relays on the network. The circuit is extended one hop at a time, and each relay along the way knows only which relay gave it data and which relay it is giving data to. No individual relay ever knows the complete path that a data packet has taken, and the client negotiates a separate set of encryption keys for each hop along the circuit to ensure that each hop can't trace these connections as they pass through. Once a circuit has been established, many kinds of data can be exchanged and several different sorts of software applications can be deployed over the *Tor* network. Because each relay sees no more than one hop in the circuit, neither an eavesdropper nor a compromised relay can use traffic analysis to link the connection's source and destination;

9. *Ultrasurf*.[17] Originally created to help Internet users in China to find security and freedom online, *Ultrasurf* is a free software that enables users to visit any public web sites in the world safely and freely through a secure encrypted connection. It is a small file (approximately 1.2 MB), and will not install anything on the computer of the user. *Ultrasurf* uses proxy technology to mask IP address at all times when using the software;
10. *Your Freedom*.[18] With about 31 servers online, in nine different countries, Your Freedom is a connectivity service that allows the user to overcome connectivity restrictions imposed upon the user by network administrators, providers or a country. It also provides a certain level of anonymization, and it hides from administrators and other people activities on the Internet. It works by turning the local personal computer into a web proxy and a SOCKS proxy that can be used by applications (web browser, games, whatever). Instead of connecting directly, applications can send connection requests to these "proxy servers" provided by the client part of the *Your Freedom* software running on the personal computer, and the client part will then forward these requests to the server part running on the company's connectivity servers through a connection protocol that is still available to the user, and through which the client part can reach the server part. It tunnels through firewalls, web proxies and, FTP proxies. The guide on the web site clearly explains that: (i) *Your Freedom* is not a VPN software,

[17] See the web site at the address http://ultrasurf.us/. Accessed 24 November 2011.

[18] See the web site at the address http://your-freedom.net/. Accessed 21 November 2011.

and it does not provide a connection to a private network, but to the Internet; (ii) *Your Freedom* is not a firewall solution, it is meant to break through firewalls, not to be one, and it does not make the personal computer of the user any safer; (iii) *Your Freedom* is not a perfect anonymizer. The service does provide a certain level of anonymization by hiding the IP address. Instead, the connection request appears to come (in fact it does come) from one of the company's connectivity server IP addresses. But it cannot protect the user from his own mistakes or flaws in applications and protocols; (iv) *Your Freedom* is not, in any way, enhancing the user's connection. It does not provide data compression and it cannot speed it up in any way; in fact, there is a certain amount of overhead which is dependent on the connectivity protocol used, so things will probably run slower, not faster. *Your Freedom* can be used to overcome: (i) Protocol restrictions: if the user cannot use certain applications or services because these applications cannot connect to the Internet in the usual way, *Your Freedom* may be able to help the user. (ii) Blacklists. Your Freedom turns the personal computer into an unrestricted web proxy that provides access to all web pages that are generally accessible. (iii) Time restrictions. Some users use Your Freedom to avoid time restrictions, starting the Your Freedom client before the restriction is in place, and keep it open.

5.4.2 *Ten Fundamental Aspects of a Typical Liberation Technology Tool*

In 2010, the hacker Roger Dingledine,[19] of the *Tor* project, drafted a brief, and really interesting, paper concerning *ten* essential requirements that a circumvention tool must have, especially if this tool is developed to bypass filters, censorship or technologies for the control (Dingledine 2010: 1).

The author, first of all, remarks that Internet-based circumvention software consists essentially of *two components*:

1. a relaying component, and
2. a discovery component (Dingledine 2010: 1).

The relaying component establishes a connection to some server or proxies, handles the encryption process, and sends traffic back and forth. The discovery component, on the other side, is the step before that: the process of finding one or more reachable addresses (Dingledine 2010: 1).

[19]See the web page of Roger Dingledine at the address http://freehaven.net/~arma/cv.html. Accessed 21 November 2011. See, also, his interesting recent studies regarding trust-based anonymous communications (Johnson et al. 2011), concerning *Tor* (Ngan et al. 2010) and on statistical data in the Tor anonymity network (Loesing et al. 2010). Of fundamental interest is, also, his paper with one of the first accurate descriptions of the Tor network (Dingledine et al. 2004) and, before Tor, of the Free Haven Project (Dingledine et al. 2000).

Dingledine notes that some tools have a very simple relaying component. He explains the example of the use of an *open proxy*, that requires only to configure the web browser or other application to use the proxy but poses, at the same time, a big *challenge*: it's not easy to find an open proxy that's reliable and fast (Dingledine 2010: 1).

On the other hand, Dingledine observes, some tools have much more sophisticated relaying components, made up of multiple proxies and multiple layers of encryption (Dingledine 2010: 1).

The hacker remarks *ten essential points* that must be present in a liberation technology tool:

1. *the tool must have a diverse set of users*. Dingledine writes that one of the simplest questions someone can ask when looking at a circumvention tool is "who else uses it". A wide variety of users means, in Dingledine's approach, that, if somebody finds out you are using the software, they can't conclude much about *why* you're using it. For example, a privacy tool like *Tor* has many different classes of users around the world (ranging from ordinary people and human rights activists to corporations, law enforcement, and militaries) so the fact that someone has *Tor* installed doesn't give people much additional information about who you are or what sorts of sites you might visit (Dingledine 2010: 1);
2. *the tool must be useful and efficient in a particular country*. The next question to consider, writes Dingledine, is whether the tool operator artificially *restricts* which countries can use it. For several years, for example, the commercial *Anonymizer.com* made its service free to people in Iran. Thus, Dingledine recalls, connections coming from *Anonymizer*'s servers were either paying customers (mostly in America) or people in Iran trying to get around their country's filters. For more recent examples, *Your Freedom*, Dingledine notes, restricts free usage to a few countries like Burma, while at times systems like *Freegate* and *Ultrasurf* outright block connections from all but the few countries that they care to serve (China and, in the case of *Ultrasurf* recently, Iran) (Dingledine 2010: 2);
3. *the tool must have a sustainable network and a software development strategy*. The tool, Dingledine observes, must ensure its *long-term existence*, especially (i) using volunteers, (ii) making a profit, and (iii) getting funds from sponsors (Dingledine 2010: 2);
4. *there must be the presence of an open design*. The first step to transparency and reusability of the tool's software and design, Dingledine remarks, is to distribute the software (not just the client-side software, but also the server-side software) *under an open source license*. It means that everyone can examine the software to see how it really operates, and has the right to modify the program. The hacker writes that even if not every user will take advantage of this opportunity (many people just want to use the tool as it is), the fact that some users can makes it much more likely that the tool will remain safe and useful. Without this option, everyone is forced to trust that a small number of developers have thought of and addressed every possible problem. There is, also, a second aspect. Just having an open source license, writes Dingledine, is not enough, because

trustworthy circumvention tools need to provide clear, complete *documentation* for other security experts: not just how it's built, but what features and goals its developers aimed for. Questions that, in Dingledine's opinion, are really important are the following: do they intend for it to provide privacy? What kind of privacy, and against what attackers? In what way does the tool use encryption? Do they intend for it to stand up to attacks from censors? What kind of attacks do they expect to resist and why will their tool resist them? Without seeing the source code and knowing what the developers meant for it to do, Dingledine concludes, it's harder to decide whether there are security problems in the tool, or to evaluate whether it will reach its goals (Dingledine 2010: 2, 3);

5. *there must be the presence of a decentralized architecture*. Another feature to look for in a circumvention tool, Dingledine writes, is whether its network is *centralized* or *decentralized*. A centralized tool, the hacker notes, puts all of its users' requests through *one* or a *few* servers that the tool operator controls. A decentralized design, like *Tor* or *JAP,* sends the traffic *through multiple different locations*, so there is no single location or entity that gets to watch what web sites each user is accessing (Dingledine 2010: 3);
6. *the tool must be untraceable*. Privacy, Dingledine remarks, isn't only about whether the tool operator can log your requests, but it's also about whether the web sites you visit can recognize or track you (and the hacker recalls the case of Yahoo turning over information about one of its Chinese webmail users). Dingledine poses some really interesting questions: what if a blog aggregator wants to find out who's posting to a blog, or who added the latest comment, or what other websites a particular blogger reads? Using a safer tool to reach the web site, the hacker suggests, means that the web site won't have as much to hand over, and, from this point of view, some circumvention tools are safer than others. Dingledine highlights two different cases: (i) at one extreme, there are open proxies, because they often pass along the address of the client with their web request, so it's easy for the web site to learn exactly where the request is coming from, but at the other extreme are (ii) tools like *Tor*, that include client-side browser extensions to hide your browser version, language preference, browser window size, time zone, and so on, or to segregate cookies, history, and cache and to prevent plugins like Flash from leaking information about you (Dingledine 2010: 4);
7. *the tool must have realistic features*. This point, in Dingledine's view, is very important, because it concerns encryption and privacy. A circumvention tool, the hacker writes, does not have to promise to magically encrypt the entire Internet, and, first of all, it is necessary to draw a distinction between *encryption* and *privacy*. Most circumvention tools (all but the really simple ones like open proxies), the scholar writes, encrypt the traffic between the user and the circumvention provider, and they need this encryption to avoid the *keyword filtering* done by such censors as China's firewall. But, Dingledine warns, none of the tools can encrypt the traffic between the provider and the destination web sites: if a destination website doesn't support encryption, there's *no magic way* to make the traffic encrypted. The ideal answer, the hacker explains, would be for

everybody to use *https* (also known as SSL) when accessing web sites, and for all web sites to support https connections. When used correctly, https provides encryption between your web browser and the web site. This "end-to-end" encryption means nobody on the network (not your ISP, not the backbone Internet providers, and not your circumvention provider) can listen in on the contents of your communication. But for a wide variety of reasons, Dingledine observes, pervasive encryption hasn't taken off. If the destination website doesn't support encryption, the best you can do is (i) not send identifying or sensitive information, such as a real name in a blog post or a password you don't want other people to learn, and then (ii) use a circumvention tool that doesn't have any trust bottlenecks that allow somebody to link you to your destinations despite the precautions in step (i) (Dingledine 2010: 4, 5);

8. *the tool must manifest good efficiency in the common use*. This more technical point, says Dingledine, regards good latency and throughput: in one word, speed. Some tools tend to be consistently fast, some consistently slow, and some provide wildly unpredictable performance. Speed, Dingledine explains, is based on many factors, including how many users the system has, what the users are doing, how much capacity there is, and whether the load is spread evenly over the network (Dingledine 2010: 4, 5);
9. *the tool must be easy and supported*. It must be easy to get the software and updates. Once a circumvention tool becomes well-known, Dingledine remarks, its web site is going to get blocked, and if it's impossible to get a copy of the tool itself, who cares how good it is? The best answer here, in the hacker's words, is to not require any specialized client software. *Psiphon*, for example, relies on a normal web browser, so it doesn't matter if the censors block their web site, and another possible approach is a tiny program like *Ultrareach* or *Freegate* that you can instant message to your friends. Option three, Dingledine concludes, is *Tor*'s *Browser Bundle*: it comes with all the software you need preconfigured, but since it includes large programs like Firefox it's harder to pass around online. In that case distribution tends to be done through social networks and USB sticks, or using Tor e-mail autoresponder that lets download Tor via *Gmail* (Dingledine 2010: 5);
10. *the tool doesn't promote itself as a circumvention tool*. Many circumvention tools, Dingledine concludes, launch with a huge media splash, but while this attention helps attract support (volunteers, profit, sponsors), the publicity also attracts the attention of the censors. Censors, the hacker remarks, generally block two categories of tools: (i) the ones that are working really well, meaning they have hundreds of thousands of users, and (ii) the ones that make a lot of noise. In many cases censorship is less about blocking all sensitive content and more about creating an atmosphere of repression so people end up self-censoring (Dingledine 2010: 6).

Dingledine concludes his fundamental analysis observing that the point is not to find the "best" tool, and having a diversity of circumvention tools in wide use increases robustness for all the tools, since censors have to tackle every strategy at once (Dingledine 2010: 6).

5.4.3 An Interesting (Comparative) Article on Real Anonimity of VPN Systems Users

In 2011, *Enigmax* of TorrentFreak (Enigmax 2011), after an alleged member of *Lulzsec* was tracked down after using a supposedly anonymous service from *HideMyAss*, published an interesting article ("Which VPN Providers Really Take Anonymity Seriously?") concerning the relationship between most common VPN services providers, log files and the anonimity of the users.

The Author wanted to know which VPN providers take privacy extremely seriously, and he asked many of the leading providers two very straightforward questions. Question 1 was: Do you keep ANY logs which would allow you or a third party to match an IP address and a time stamp to a user of your service? If so, exactly what information do you hold?

Question 2 was: Under what jurisdictions does your company operate and under what exact circumstances will you share the information you hold with a third party? The Author notes that, if a VPN provider carries logs of their users' activities, the chances of them being able to live up to their claim of offering an anonymous service begins to decrease rapidly.

He then contacted "some of the leading, most-advertised, and most talked about VPN providers in the file-sharing and anonymity space", interested in knowing if the offered services are 100% anonymous.

Here is a brief "map" of the conclusions for each company contacted:

1. *BTguard*: Q1: "It's technically unfeasible for us to maintain log files with the amount of connections we route. We estimate the capacity needed to store log files would be 4 TB per day." Q2: "The jurisdiction is Canada. Since we do not have log files, we have no information to share. We do not communicate with any third parties. The only event we would even communicate with a third party is if we received a court order. We would then be forced to notify them we have no information. This has not happened yet."
2. *Private Internet Access*: Q1: "We absolutely do not maintain any VPN logs of any kind. We utilize shared IP addresses rather than dynamic or static IPs, so it is not possible to match a user to an external IP. These are some of the many solutions we have implemented to enable the strongest levels of anonymity amongst VPN services. Further, we would like to encourage our users to use an anonymous e-mail and pay with Bitcoins to ensure even higher levels of anonymity should it be required." Q2: "Our company currently operates out of the United States with gigabit gateways in the US, Canada, UK, Switzerland, and the Netherlands. We chose the US, since it is one of the only countries without a mandatory data retention law. We will not share any information with third parties without a valid court order. With that said, it is impossible to match a user to any activity on our system since we utilize shared IPs and maintain absolutely no logs."
3. *TorrentPrivacy*: Q1: "We have connection logs, but we don't store IP addresses there. These logs are kept for 7 days. Though it's impossible to determine who exactly have used the service." Q2: "We have servers in Netherlands, Sweden

and USA while our company is based on Seychelles. We do not disclose any information to third parties and this can be done only in case of a certain lawsuit filed against our company."

4. *TorGuard*: Q1: "Our sever connection logs are purged on a daily basis since we don't maintain hard drive's big enough to store all this data. TorGuard's torrent proxy and VPN connection logs do not associate an IP with each request as there are hundreds of users sharing the same connection at any given time. Since there are no logs kept or IP's recorded, it is not possible to identify exactly who has used the connection." Q2: "Our parent company is based in Panema, with secure servers in Netherlands, Romania, Ukraine and Panema. We do not share any of our user's information with third parties, period. Only in the event of an official court order would we be forced to communicate with a third party. This scenario has never occurred, but if it were to, we would be forced to explain in more technical terms how we don't maintain usage logs."
5. *ItsHidden*: Q1: "No logs, they are not kept. Even system logs that do not directly link to users are rotated on an hourly basis." Q2: "The company has recently been sold and falls under the Jurisdiction of the Seychelles. As such there is no requirement to log within that jurisdiction."
6. *Ipredator*: Q1: "We don't store the IP at all actually. It's in temporary use for the session you have when you're connected but that's it. We've had very few issues with not having logs, but not keeping them makes it safer even for us since we can't accidentally give out information about anyone". Q2: "We fall – mostly – under Swedish jurisdiction when it comes to the service. When it comes to organisational stuff (who keeps the data, who owns the service, who owns the server, who owns the network etc. etc.) it's very mixed, intentionally. This is to make it hard and/or impossible to legally bully us around if that would be the case." "We can't be easily shut down, and we can't be pressured by courts to implement stuff we would oppose. For end-users this is not affecting them in a negative way at all, only the opposite."
7. *Faceless*: Q1: "We do not log any IP addresses and no information about what data is accessed by our users, so we have no information that could be interesting to third-parties." Q2: "We have servers in The Netherlands and our company is based in Cyprus. If authorities would contact us we would have to tell them that we have no connection logs or IP-addresses saved on our systems."
8. *IPVanish*: Q1: We in no way record or store any user's activity while connected to IPVanish. The only information we collect from a VPN session is: Timestamp (date and server time) of the connection to us, duration of the connection, IP address used for the connection and bytes transferred. Logs are also regularly cycled. Additionally, IPVanish users are given dynamic and SHARED IP addresses on the same servers – making it impossible for us to single out anyone for anything. Q2: "We operate out of the US and, like all companies and citizens, must comply with local law. As detailed earlier, we have generic connection logs, but that information is not sufficient for identifying individual users. We take privacy and reliable extremely seriously and will also never share, rent or lease any information to any third party."

9. *AirVPN*: Q1: The company carries no identifying logs. Q2: "Jurisdiction is in the EU, under most circumstances Italy (country of the company and home of the person legally responsible for data protection), but applicable law may be one of the EU Member States where the servers of the network are physically located (no servers are in Italy)," AirVPN told us. "We don't share any information with anyone."
10. *PRQ*: "We do not log anything, not even temporary logs. We do not have any "personal information", since we only require a working e-mail address to sign up. Many customers use anonymous e-mail services like hushmail and the like. Even if a customer gives us their information, we do not use it." Q2: "We fall under Swedish jurisdiction, no circumstances will be accepted to share information, since we do not have any information to share."
11. *VPNReactor*: Q1: "Only for 5 days to stop abuse […] After 5 days we have absolutely no way to match any IP address or time stamp to any users. Privacy and Security is further enhanced for individual users because their VPN connections are basically lost in the crowd." "Our free VPN users share a block of IPs when they connect to the internet via VPNReactor. So at any given time hundreds/thousands of our VPN users that have active connections could all be sharing a single IP address. None of our VPN users are assigned individual public IPs." Q2: "We strive to be upfront and transparent with our logging policies for the benefit of our VPN users." Logs seen by TorrentFreak seemed to confirm no identifiable information being stored. "We are a U.S. based company and are bound by U.S. based court orders […] However, if a U.S. based subpoena comes in requesting info for activity that occurred more then 5 days prior, we have absolutely nothing to provide as our logs would have expired off. Request for connection details outside a U.S. based court order will be fully ignored."
12. *BlackVPN*: Q1: "We do not keep any logs about our users internet activities including which sites they access or what data they transfer. We also run log cleaners on our systems which removes the IPs from logs before they are written to disk" "For tax and legal reasons we do store some billing information (name, email, country), but it is stored with a third-party and separate from the rest of BlackVPN." BlackVPN say they hold a username and email address of their subscribers and the times of connection and disconnection to their services along with bandwidth consumption. Logging is carried out as follows: "On our Privacy Servers, NL & LT we don't log anything that can identify the user, but on our US & UK server where we don't allow sharing copyrighted materials we do log the internal RFC1918 IP that is assigned to the user at a specific time," BlackVPN explain. "So to clarify, we don't log the real external IP of the user, just our RFC1918 internal one, this we have to do to comply with local laws and to be able to handle DMCAs." Update: in their FAQ BlackVPN now writes: "Although we do not monitor the traffic, incoming or outgoing connections of our users we may assign users to a unique IP address and log which user was assigned which IP address at a given time. If we receive a copyright violation notice from the appropriate copyright holder then we will forward the violation

to the offending user and may terminate their account. We therefore ask our users not to distribute or transmit material which violates the copyright laws in either your country or the country in which our Service is hosted." Q2: "We operate under the jurisdiction of the Netherlands and we will fiercely protect the privacy and rights of our users and we will not disclose any information on our users to anyone, unless forced to by law enforcement personnel that have produced the proper legal compliance documents or a court order. (In which case we don't really have a choice)."

13. *PrivatVPN*: Q1: "We don't keep ANY logs that allow us or a third party to match an IP address and a time stamp to a user our service. The only thing we log are e-mails and usernames but it's not possible to bind a activity on the Internet to a user." Please note: PrivatVPN also offer use of a US server for watching services like Hulu. IP logs are kept when users use this service. Q2: "Since we do not log any IP addresses [we have] nothing to disclose. Circumstances doesn't matter in this case, we have no information regarding our customers' IP addresses."
14. *Privacy.io*: Q1: "No logs whatsoever are kept. We therefore simply are not able to hand data out. We believe that if you are not required to have logs, then you shouldn't. It can only cause issues as seen with the many data leaks in recent years. Should legislation change in the juristictions we operate in, then we'll move. And if that's not possible, then we'll shut the service down. No compromises." Q2: "We span several jurisdictions to make our service less prone for legal attacks. Servers are currently located in Sweden. We do not share data because we don't have it. We built this system because we believe only when communicating anonymously, you can really freely express yourself. As soon as you make a compromise, you are going down a slippery slope to surveillance. People will ask for more and more data retention as seen around the world in many countries recently. We do it because we believe in this, and not for the money."
15. *Mullvad*: Q1: "No. And we don't see why anyone would. It would be dishonest towards our customers and mean *more* potential legal trouble." Q2: "Swedish jurisdiction. We don't know of any way in which the Swedish state in practice could make us behave badly towards our clients and that has never happened. Another sign we take privacy seriously is that we accept payments in Bitcoin and cash in the mail."
16. Cryptocloud: Q1: "We log nothing at all." Q2: "We don't log anything on the customer usage side so there are no dots to connect period, we completely separate the payment information," they told us. "Realistically unless you operate out of one of the 'Axis of Evil Countries' Law Enforcement will find a way to put the screws to you," Cryptocloud add. "I have read the nonsense that being in Europe will protect you from US Law Enforcement, worked well for HMA didn't it? Furthermore I am pretty sure the Swiss Banking veil was penetrated and historically that is more defend-able than individual privacy. The way to solve this is just not to log, period."
    The is also a list of VPN providers who log.

17. *VyprVPN* is the VPN service connected to and offered by the Giganews Usenet service, although it can be used completely standalone. In common with many other providers contacted, VyprVPN acknowledged receipt of the two questions but then failed to respond. The company policy says that logging data "is maintained for use with billing, troubleshooting, service offering evaluation, [Terms of Service] issues, [Acceptable Use Policy] issues, and for handling crimes performed over the service. We maintain this level of information on a per-session basis for at least 90 days." On Usenet forum NZBMatrix several users have reported having their VyprVPN service terminated after the company processed "a backlog" of DMCA notices which pushed them over the "two-strikes-and-out" acceptable use policy.
18. *SwissVPN*: they are well known, relatively cheap and have been used by those on a tight budget. To their credit, they were also the fastest company to respond. They are one of the few companies that do not make anonymity claims. Q1: "SwissVPN is being operated based on Swiss Telecommunications and Personal Data Protection Law. Session IP's (not visited content, websites, mail, etc.) are being logged for 6 months," the company told us. Q2: The company responds to requests from third parties under Swiss criminal law.
19. *StrongVPN* This company did not directly answer questions but pointed to their logkeeping policy instead. StrongVPN do log and are able to match an external IP address to their subscribers. They were the most outwardly aggressive provider in the survey when it came to dealing with infringement. "StrongVPN does not restrict P2P usage, but please note sharing of Copyrighted materials is forbidden, please do not do this or we will have to take action against your account" "StrongVPN Notice: You may NOT distribute copyright-protected material through our network. We may cancel your account if that happens."

References

Copeland, D. 2012. How to get around the great firewall of China. http://www.readwriteweb.com/archives/how-to-get-around-the-great-firewall-of-china.php?utm_source=ReadWriteWeb+Newsletters&utm_medium=email&utm_campaign=dfd3f8bc22-RWWDailyNewsletter. Accessed 12 June 2012.

Dingledine, Roger. 2010. Ten things to look for in a circumvention tool. https://www.torproject.org/press/presskit/2010-09-16-circumvention-features.pdf. Accessed 24 Nov 2011.

Dingledine, Roger, Michael J. Freedman, and David Molnar. 2000. The free haven project: distributed anonymous storage service. http://www.cs.princeton.edu/~mfreed/docs/freehaven-pet00.pdf. Accessed 24 Nov 2011.

Dingledine, Roger, Nick Mathewson, and Paul Syverson. 2004. Tor: The second-generation onion router. https://svn.torproject.org/svn/projects/design-paper/tor-design.pdf. Accessed 24 Nov 2011.

Enigmax. 2011. Which VPN providers really take anonymity seriously? https://torrentfreak.com/which-vpn-providers-really-take-anonymity-seriously-111007/. Accessed 10 June 2012.

Grimmelmann, James. 2012. Sealand, HavenCo, and the rule of law. http://works.bepress.com/cgi/viewcontent.cgi?article=1035&context=james_grimmelmann. Accessed 13 Nov 2012.

Johnson, Aaron, Paul Syverson, Roger Dingledine, and Nick Mathewson. 2011. Trust-based anonymous communication: Adversary models and routing algorithms. http://freehaven.net/~arma/anonymity-trust-ccs2011.pdf. Accessed 21 Nov 2011.

Loesing, Karsten, Steven Murdoch, and Roger Dingledine. 2010. A case study on measuring statistical data in the Tor anonymity network. Workshop on ethics in computer security research. http://www.cl.cam.ac.uk/~sjm217/papers/wecsr10measuring.pdf. Accessed 24 Nov 2011.

Ngan, Tsuen-Wan "Johnny", Dingledine, Roger, and Wallach, Dan S. 2010. Building incentives into Tor. Financial cryptography and data security. http://freehaven.net/anonbib/papers/incentives-fc10.pdf. Accessed 24 Nov 2011.

Roberts, Hal, Ethan Zuckerman, Jillian York, Robert Faris, and John Palfrey. 2010. Circumvention tool usage report. http://cyber.law.harvard.edu/sites/cyber.law.harvard.edu/files/2010_Circumvention_Tool_Usage_Report.pdf. Accessed 24 Nov 2011.

Chapter 6
Digital Activism, Internet Control, Transparency, Censorship, Surveillance and Human Rights: An International Perspective

6.1 An Introductory Overview

6.1.1 The Global OpenNet Initiative Analysis

The *OpenNet Initiative* (ONI)[1] has sought to provide a preliminary study (*Regional Overviews*), based on macro-regions and continent,[2] in order to create a comprehensive, worldwide assessment of the *levels* of censorship, surveillance and restrictions of digital liberties. The study, after a preliminary introduction, goes on to provide a first, interesting analysis of the development of digital liberties in individual countries.

It therefore seems appropriate, before commencing with a fairly in-depth exploration and analysis of the legislation, the technological landscapes and the political frameworks of a number of "key" countries (in terms of *human rights* and *digital freedoms* issues) to briefly summarize the status of digital freedoms in all the regions of the world based on the series of studies conducted by this active organization.

The first geographical area that is described in the ONI *Report* is that currently considered to be the most problematic: *Asia*. Many nations, in Asia, have seen spectacular diffusion of the use of technology, which has, in numerous areas, rapidly lead to significant increases in the rate of local economic growth as well.[3]

---

[1] See the official web site at http://opennet.net/. Accessed 19 November 2011.

[2] See the full text of the *Report* at http://opennet.net/research/regions. Accessed 15 November 2011. The authors of the *Report* write, on the ONI web site: "The eight regional overviews provide broad summaries that exhibit the ways in which the countries within each region are grappling with the implications of *Internet freedom* and the challenges of *regulating online content*. These overviews include background research and, when applicable, synthesize the findings of *technical tests* carried out in these regions" (emphasis mine).

[3] See Asiatic Internet usage and population statistics (updated for June 30, 2011), at http://www.internetworldstats.com/stats3.htm. Accessed 26 November 2011. According to these statistics, Asia (with a population, in 2011, of 3,879,740,877) has an Internet penetration rate of 24% (932,393,209 Internet users, and 152,957,480 *Facebook* subscribers) and has the 56% of the

G. Ziccardi, *Resistance, Liberation Technology and Human Rights in the Digital Age*, Law, Governance and Technology Series 7,
DOI 10.1007/978-94-007-5276-4_6, © Springer Netherlands 2013

China,[4] Burma[5] and Vietnam[6] are, according to the ONI *Report*, the three countries relying most significantly on pervasive Internet filtering practices, targeting political and cultural content. Four most frequent *targets* are:

1. sites hosting articles in local languages;
2. sites and articles relating to human rights coverage;
3. independent news sources; and
4. topics such as discrimination against ethnic and religious minorities and activists.

Singapore,[7] on the other hand, is more concerned with blocking sites considered to be *pornographic* or featuring *adult content*.

With regard to the Internet and political control in Singapore, an enlightening essay by Rodan clearly indicates that Singapore poses a fascinating case-study. As the author explains (emphasis mine):

> Here we have one of the most comprehensive strategies for the development of IT anywhere in the world, supported by huge state-led infrastructure investments. Indeed, Singapore's policy makers are committed to the transformation of the island economy into an information hub, trading in ideas rather than commodities. Yet Singapore's authoritarian leaders have no intention of surrendering political control in the process […] Although the Internet represents a more difficult technical challenge for Singapore's control-minded officials, the government has embarked on an ambitious attempt to superimpose *strict broadcasting censorship* on the medium (Rodan 1998: 64, 65).

Rodan also remarks that Singapore's authorities demonstrated their technical capacity to monitor usage of the Internet on more than one occasion. In 1994, a scan of public Internet accounts held with the local ISP *Technet*, conducted during a search of graphic files, produced a total of 80,000 files, of which *five* were considered, by authorities, to be pornographic (Rodan 1998: 76). The author correctly observes that the demonstration of state capabilities for searching files on a vast scale may, in itself and by design, have a suitably *chilling effect* (Rodan 1998: 77).

---

population of the world. For a complete overview of Internet governance, intended as (emphasis mine), " […] 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" (Butt 2005: 2), in Asia and in 27 countries of the region, see the study by Butt regarding information and communications technology strategies and the public policy issues in these regions (Butt 2005). See, also, the Deibert, Palfrey, Rohozinski and Zittrain study regarding security, identity, and resistance in Asian Cyberspace (Deibert et al. 2012).

[4] See the ONI *Country Profile* regarding China at http://opennet.net/research/profiles/china-including-hong-kong. Accessed 21 November 2011. See, also, Sect. 6.2.7.

[5] See the ONI *Country Profile* regarding Burma at http://opennet.net/research/profiles/myanmar-burma. Accessed 21 November 2011. See, also, Sect. 6.2.1.

[6] See the ONI Country Profile regarding Vietnam at http://opennet.net/research/profiles/vietnam. Accessed 21 November 2011. See, also, Sect. 6.2.10.

[7] See the ONI Country Profile regarding Singapore at http://opennet.net/research/profiles/singapore. Accessed 24 November 2011.

South Korea[8] actively filters pornographic content, web sites containing North Korean propaganda or relating to the fairly volatile topic of the reunification of the two countries, and additionally blocks a number of gambling web sites.[9] In Pakistan,[10] there have been only occasional episodes of filtering of pornography or religious web sites, although there has been a considerable increase in the censorship of sites containing material considered to be *blasphemous*. Indonesia, Laos, Nepal,[11] the Philippines, Bangladesh and Malaysia[12] have blocked some sites for short periods, but ONI observes that there is no evidence of systematic action such as that of the states discussed above.

In 2012, in Malaysia, the Prime Minister Datuk Seri Utama Dr Rais Yatimand expressed support for Tun Dr Mahathir Mohamad's (information, communications and culture Minister) call for regulations to control the absolute freedom that exists on the Internet and agreed that the "cyberworld should now be subjected to perusal by society". The Minister cited cheating, gambling, phishing for particulars and spreading pornography on the Internet as criminal offences and "therefore to disregard this purely for sake of freedom on the Internet is not a true thing". "The principle we must recognise" – he said – " is that the laws of the land must be respected […] If the laws are enforced, it doesn't mean that we are censoring the Internet […] Countries should now enforce some form of regulatory control to block "filth" and punish those who corrupt the minds of Internet users" (Ariffin 2012).

Except filtering issues, in Malaysia, in 2012, passed an amendment to The Evidence Act that clearly signals the government's intention to increase censorship on the internet. As Kee noted (Kee 2012) "The amended act is deeply problematic at several levels and directly counters fundamental democratic principles […] At the most basic level, the newly introduced Section 114(A) to the Evidence (Amendment) (No 2) Act 2012 has the impact of removing the critical presumption

[8] See the ONI *Country Profile* concerning South Korea at http://opennet.net/research/profiles/south-korea. See, also, Sect. 6.2.3.

[9] See, also, Sect. 6.2.15.

[10] See the ONI *Country Profile* regarding Pakistan at http://opennet.net/research/profiles/pakistan. Accessed 21 November 2011.

[11] See the ONI *Country Profile* regarding Nepal at http://opennet.net/research/profiles/nepal. Accessed 21 November 2011.

[12] See the ONI Country Profile concerning Malaysia at http://opennet.net/research/profiles/malaysia. Accessed 21 November 2011. For an interesting technological and political overview see, also, Gong's study regarding Internet politics, state controls and the effect of blogs on the 2008 general election in Malaysia (Gong 2011). The author described how opposition candidates benefited significantly more from having *a blog* than did non-opposition candidates, as blogging provided opportunities denied to them by Malaysia's state-controlled media (Gong 2011: 307). According to Gong, two points are, in similar situations, fundamental: (i) the Internet allows previously marginalized, or even new parties, to *emerge* and *compete* with established players especially in Malaysia, where the opposition is denied easy access to mainstream media and where the Internet becomes a *powerful means* they can use to gain publicity; (ii) there is a potential redistribution of power, and egalitarian use of the Internet may result in *decentralized networks* that *redistribute power* from party leaderships to grassroots activists (Gong 2011: 311–312).

of innocence principle, which is at the cornerstone of our criminal justice system. This principle protects individuals against wrongful conviction, by ensuring that everyone has access to a fair trial. It also upholds the ideal that every person is a law abiding citizen until proven otherwise, and provides an important safeguard against abuse of power by the government to persecute individuals by requiring any allegations to be proven beyond reasonable doubt. If this amended law were to take effect, all 17 million internet users in Malaysia who post anything online – from emails to comments to status updates – will exist in a state of presumed illegality. Instead of being law abiding citizens, we are all instead assumed to be criminals unless we can prove otherwise. […] Datuk Seri Nazri Abdul Aziz from the Prime Minister's Department justified the need for such an amendment to overcome the difficulty of anonymity and pseudonyms in cybercrime cases. […] The amendments to the Evidence Act […] (places) blanket assumptions of criminal liability upon all internet users who use the internet for information exchange and expression, including those who host websites which allow for interaction with users, e.g. comment boxes. This law will promote a feeling of fear amongst internet users and result in occurrences such as website owners removing comment functions – which is a key characteristic of the internet today as a vibrant, interactive public space for democratic deliberations". (Kee 2012).

The newly included Section 114A to the Malaysian Law provides that: (i) a person whose name, photograph or pseudonym appears on any publication depicting himself as the owner, host, administrator, editor or sub-editor, or who in any manner facilitates to publish or re-publish the publication is presumed to have published or re-published the contents of the publication unless the contrary is proved; (ii) a person who is registered with a network service provider as a subscriber of a network service on which any publication originates from is presumed to be the person who published or re-published the publication unless the contrary is proved; (iii) Any person who has in his custody or control any computer on which any publication originates from is presumed to have published or re-published the content of the publication unless the contrary is proved. (Computer here means any data processing device, including tablets, laptops and mobile phones.) (Kee 2012).

An interesting Hill's analysis of East Timor and the Internet, and of global political leverage in Indonesia (Hill 2002), examines how one particularly marginalized regional *independence movement* has exploited the potential of the Internet in its struggle, and how the Internet enabled pro-East Timor activists from around the world to work collectively, coordinating closely with East Timorese leaders both inside the occupied territory and in exile, in a focused, accurate manner only previously achieved by governments or by large international corporations. East Timor provides, according to the author, a striking example of how a protracted independence struggle, adjusted to the new strategic possibilities of the Internet, could exert *international political leverage*, and how they can be applied by a nation on the *path to independence* (Hill 2002: 26). Hill's conclusions are clear (emphasis mine):

> For some supporters at least, the very newness and capacity of the medium itself, with the startling advances in communication it offered, engendered *a new confidence* in their own capacity to organize and mobilize support. The speed, currency, and volume of

> communication that the internet offered gave activists their own 'mass medium' which, in turn, encouraged greater activist response Once information – even a snippet smuggled by an individual out of East Timor – was fed into this electronic network, it became *further ammunition* in the global battle for public opinion. In the commercial media, 'accounts of the suffering of the Timorese were sporadic, and rarely came into sharp and sustained focus'. By contrast, electronic networking, made possible by internet technology, assisted in maintaining nodes of informed activists and, beyond them, a broader 'group of sympathisers ready to respond if and when some development re-ignited the issue'. […] It was a *power* mobilized to unanticipated effect by supporters of an independent East Timor. But it was not the technology of the internet that sustained an international campaign for East Timor. The technology was simply employed by activists who would (and did), in its absence, struggle to gain and wield diplomatic and political leverage, using *whatever technologies were at their disposal*. In this articulation with a range of other technologies – 'new' and 'old' – the internet takes its place as a powerful tool in the service of civil society (Hill 2002: 34, 49).

Concerning Indonesia, and the use of the Internet for activism and dissidence, similar conclusions are reached in another study regarding *crackdowns* in that country (Randall 1996). The author remarks that it is not necessary to *exaggerate* the democratic potential of the Internet to recognize that it has created an *open forum* for the expression of ideas of a kind not available to Indonesians for some decades, underground leaflets aside (Randall 1996: 38).

It should be noted that Asia is characterized, on the one hand, by states, such as China, with high Internet penetration rates and the greatest number of individual users on the planet, and, on the other hand, by nations such as Nepal, which are still, in large part, disconnected and profoundly affected by the digital divide, for reasons that are not only cultural but also geographical.[13]

In Nepal, where only 1% of the population has access to the Internet, the *Nepal Wireless* project is overcoming these barriers by connecting several villages to the Internet.[14]

Burma, however, we will see,[15] was the theater of one of the most severe and bloody *crackdowns* on the Internet of the modern age: the military government, on 29 September 2007, aiming to cut off the stream of footage and images of the violent response by the military to protests lead by monks and civil activists, shut down the Internet and all web access across the entire country, with only intermittent periods of connectivity, for approximately 2 weeks. User upload speeds were also halved by the government, in order to limit the transmission of information

[13] See Sect. 1.4.

[14] See the official web site of the project at http://www.nepalwireless.net/. Accessed 21 November 2011. As is remarked on the web site of the project, this action is inspired by the social cause for the socio economic transformation of rural villages in Nepal by optimum use of Information and Communication technologies, and is promoting wireless technologies connecting rural side to urban areas so that the transfer of technologies from urban to rural area would be possible through Internet and Intranet. Nepal Wireless have received license from Nepal Telecommunication Authority for wireless frequency of 5.8 GHz and 2.4 GHz through ISM band, and is planning to bring Internet to several sectors, like (i) e.commerce, (ii) tele-medicine, and (iii) distance learning.

[15] See Sect. 6.2.1.

over the web. The facts, by now, are well-known, but it might all the same be worthwhile to present them again: on August 19, 2007 the leaders of the student movement *88 Generation* organized a protest against an increase in fuel prices in Rangoon. In the following months, the protest grew to include Buddhist monks, with a participation in the movement, on 23 September of the same year, of over 150,000 people. After the first days of the regime's violent repression, a number of journalists, activists and hackers began to feed the web with images, videos and reports that soon reached both Internet users and newspaper headlines around the world. This flow of critical information from the country was purposely posted to well-known overseas sites which then fed the same data back into the country via satellite television and radio. This created a bi-directional flow of vital information, interrupted only when the government proceeded to completely shutdown the Internet throughout the country.

Digital activists have been at work in other Asian nations as well. In Malaysia, independent news sites and blogs were credited with providing opposition parties with a platform to mobilize during the March 2008 elections, in which five dissident bloggers were elected to seats in Parliament. In November 2007, the President of Pakistan, Pervez Musharraf, declared a state of emergency and *shut down* all traditional news media channels; however, in response to this political move, all radio and television channels swiftly went online, and continued to document protests activities on *YouTube*.

It is important to note that such situations, which in many ways may appear almost surreal, are in many nations often facilitated by a legal framework *specifically designed* to enable the repression of dissidents and of those who in any way oppose the government. In Thailand,[16] in March 2009, citing several dispositions of the 2007 *Computer Crimes Act*,[17] police arrested Chiranuch Premchaiporn, the director and moderator of the site *Prachathai.com*, for allegedly having allowed controversial comments regarding the Thai royal family to remain on the site for 20 days. In fact, throughout Asia and throughout the world, many laws aiming to punish computer crimes are, unfortunately, also used against citizen journalists. In 2012, on May 30, the Bangkok Criminal Court found Chiranuch Premchaiporn guilty of computer crimes and sentenced her to 1 year in

[16] See the ONI *Country Profile* regarding Thailand at http://opennet.net/research/profiles/thailand. Accessed 14 November 2011.

[17] See an English translation of the *Computer Crimes Act* at http://www.prachatai.com/english/node/117. Accessed 19 November 2011. See, especially, *Section 16* of the Act, which states (emphasis mine): "Any person, who imports to a computer system that is publicly accessible, computer data where a third party's picture appears either created, edited, added or adapted by electronic means or otherwise *in a manner that is likely to impair that third party's reputation or cause that third party to be isolated, disgusted or embarrassed,* shall be subject to imprisonment for not longer than 3 years or a fine of not more than 60,000 baht, or both. If the commission under paragraph one is a trustworthy action the perpetrator is not guilty. An offence under paragraph one shall be a compoundable offence. If a party injured by an offence under paragraph one has died before filing a complaint, then their parents, spouse or children may file a complaint and shall be deemed to be the injured party".

prison, which the Court then reduced to 8 months and suspended. As Human Rights Watch reported (HRW 2012):

> By convicting the manager of a news website of a crime, the Thai authorities are showing the lengths they are willing to go to stifle free expression […] More and more web moderators and internet service providers will censor discussions about the monarchy out of fear they too may be prosecuted for other people's comments. Police arrested Chiranuch on March 6, 2009 during the crackdown on online media with content that the government considered offensive to the monarchy initiated by the government of then-prime minister Abhisit Vejjajiva. She was charged under the Penal Code and the Computer Crimes Act as an internet service provider, or intermediary, for 10 alleged *lese majeste* statements posted by others on the Prachatai web-board between April and November 2008. Under Thailand's Penal Code, breaches of lese majeste – insulting the monarchy – are considered threats to national security. Internet service providers are required to promptly remove any content deemed offensive to the monarchy and turn over details of those who post such content when requested by the authorities. The Computer Crimes Act provides that any service provider "intentionally supporting or consenting" to posting of unlawful content is subject to the same penalty imposed on the poster, which is a maximum imprisonment of five years per offense. Holding internet service providers liable is a particularly pernicious practice that makes third parties responsible for the content of others, effectively turning them into the enforcers and censors for the government […] Since the September 2006 coup, Thai authorities have increasingly applied lese majeste laws, under the Penal Code and the Computer Crimes Act, to anyone alleged to have criticized the monarchy. Despite its promises to restore respect for human rights in Thailand, the government of Prime Minister Yingluck Shinawatra, which took office in August 2011, has shown little interest in ending lese majeste crackdowns initially launched by previous governments. Deputy Prime Minister Chalerm Yubamrung told the Parliament on August 26, 2011 that lese majeste "will not be allowed during this government." In December the government established a so-called "war room" at police headquarters in Bangkok to supervise the surveillance on lese majeste websites. Since then, more than 5,000 webpages (URLs) with alleged lese majeste content have been shut down (HRW 2012).

With regard to Oceania, and specifically to Australia and New Zealand,[18] the *OpenNet Initiative* study on this area reveals that it is the former of these two nations to have the more restrictive practices.

In Australia,[19] the Constitution does not explicitly give the right to free speech, while, at the same time, it does grant the government wide *communications powers*, which have been utilized by Australian authorities to regulate offensive content on the web, creating a government body with the power to issue take-down notices for any content deemed inappropriate on any site hosted within the country. In Australia there is, also, an opt-in filtering system, in which users voluntarily accept filtering software that blocks offensive material hosted outside the country.

In ex-Soviet Union countries,[20] as described in the *OpenNet Initiative*'s research, the situation regarding digital freedoms is somewhat more *complex* than in many

[18] See the ONI *Regional Overview* concerning Australia and New Zealand at http://opennet.net/research/regions/australia-and-new-zealand. Accessed 24 November 2011.

[19] See, also, Sect. 6.2.11.

[20] See the ONI Regional Overview regarding Commonwealth of Independent States at http://opennet.net/research/regions/commonwealth-independent-states. Accessed 24 November 2011.

other areas. The traditions of *authoritarianism*, of *media control* and of the *lack of individual rights* might be, at first glance, the ideal terrain for wide-spread and pervasive restriction and regulation. In reality, however, the situation varies enormously from country to country. Some nations, for example, clearly seek to utilize the Internet as a means of developing their economies, further developing their formidable experience in the fields of mathematics, cryptography and cryptoanalysis. At the same time, however, there is the fear that the Internet might aid and encourage resistance and opposition activities. In the Ukraine,[21] Georgia[22] and Kyrgyzstan,[23] technology has lead to the discovery of *electoral fraud* and allowed official election results to be successfully challenged.

Goldstein, in 2007, drafted a case-study regarding the role of digital networked technologies in the Ukrainian 2004 *Orange Revolution* (Goldstein 2007). The author describes, in the first portion of his study, the activities of online *citizen journalists*, in their action of reporting many stories not covered by mainstream media and, in the second portion, the use of technologies during the organization of pro-democracy activities. The scholar concludes his study with two interesting statements:

1. technologies render a wide range of activities *easier* (Goldstein 2007: 2), and
2. the willingness of activists and journalists to *take risks* in their activities was of fundamental importance (Goldstein 2007: 2).

Goldstein also notes that the *Orange Revolution* registered a great use of *digital tools*, with a broad range of uses, from the coordination of activists via SMS to the development of an independent media system and a nearly completely online alternative media environment, for the reporting of election frauds (Goldstein 2007: 3). With regard to how communication technologies influenced the events in the Ukraine, the author writes (emphasis mine):

> While a *wide range of factors* shaped the events and outcomes of the Orange Revolution, the Internet and mobile phones proved to be *effective tools* for *pro-democracy* activists. First, the Internet allowed for the creation of a *space* for dissenting opinions of 'citizen journalists' in an otherwise self-censored media environment. Second, pro-democracy activists used the convergence of mobile phones and the Internet to *coordinate* a wide range of activities including election monitoring and large-scale protests. It is worth stating that few observers would argue that the Orange Revolution would not have happened without the Internet. Moreover, given the multiplicity of factors in play during a political revolution, it is not appropriate to infer that in similar circumstances the application of technology will lead to the same outcome as in Ukraine. However, in the case of Ukraine it is evident that pro-democracy forces used the Internet and cell phones more effectively than the pro-government forces, such that in this specific time and place these technologies weighed in on the side of democracy (Goldstein 2007: 9).

[21] See the ONI *Country Profile* concerning Ukraine at http://opennet.net/research/profiles/ukraine. Accessed 24 November 2011.

[22] See the ONI *Country Profile* concerning Georgia at http://opennet.net/research/profiles/georgia. Accessed 24 November 2011.

[23] See the ONI *Country Profile* concerning Kyrgyzstan at http://opennet.net/research/profiles/kyrgyzstan. Accessed 24 November 2011.

ONI reports remarks that 8 of the 11 ex-Soviet Union states have implemented *content filtering systems*, and there has been a concomitant flourishing of laws aiming to restrict the free exchange of information, especially with regard to *bloggers* and the *independent press*, with particular attention to political news and to any criticism of the government. Added to this, in many states, governments require all web sites to be registered with authorities, in the same fashion as traditional mass media are registered.

Even Europe, according to the *OpenNet Initiative* reports on this region, is not immune to restrictive Internet policies and practices.[24] The greatest attention is placed on *child pornography*, *racism*, *hate crimes* and *terrorism*, to which is added, in many states, further attention to cases of *copyright violation* and *online gambling*. Some countries, such as the United Kingdom, have been criticized for the widespread practice of notice-and-take-down, which considerably conditions the freedom of speech in that country, but which Internet Service Providers have adopted without significant difficulties. In Europe, however, more common than systematic and diffused filtering are distinct episodes of *specific* content filtering and blocking.

An interesting study by Vedres, Bruszt and Stark concerning *organizing technologies* in Europe (Vedres et al. 2005) focused on *forms of online civic associations* in Eastern Europe, collecting data on 1,585 East European civil society web sites and identifying *five* emergent genres of organizing technologies: (i) newsletters, (ii) interactive platforms, (iii) multilingual solicitations, (iv) directories, and (v) brochures (Vedres et al. 2005: 171).

As the authors remark, the post-socialist societies of Eastern Europe provide an extraordinary *laboratory* for exploring the coevolution of organizational forms and interactive technology. Not only the emergence of voluntary associations in the region coincides with the digital revolution, but it is possible, the authors explain, to draw a precise timeline:

1. *situation before 1989*. Prior to 1989, the scholars note, there were almost no non-governmental organizations in the conventional sense in Eastern Europe, and the Internet was in its infancy. Before 1989, the small number of beleaguered voluntary associations communicated by *samizdat*. With no access to photocopy machines, activists attached special springs to typewriter keys to produce up to seven carbon copies of their documents. In Prague, for example, it was not uncommon for the members of an underground philosophy seminar to circulate texts that were literally in *manuscript*, some in the handwriting of elementary school children who had painstakingly copied a parent's writings so it could circulate more widely (Vedres et al. 2005: 174);
2. *situation in modern times*. Today, the authors observe, both NGOs and the Internet are experiencing *exponential growth* throughout the region. In Hungary, for example, the number of NGOs jumped to about 15,000 in the first year after

[24] See the ONI *Regional Overview* regarding Europe at http://opennet.net/research/regions/europe. Accessed 24 November 2011.

> the democratic transition and now stands at more than 50,000, while at the same time, by conservative estimates, the number of people online doubles every year, and the number of web sites doubles every 6 months. In little more than a decade, the scholars remark, the technological framework in which voluntary associations are operating has gone from the limitations of a pre Gutenberg setting to the opportunities of advanced communication technologies (Vedres et al. 2005: 174).

In Latin America,[25] with the notable exception of Cuba,[26] the situation is somewhat less worrisome. Constant attention is paid to the repression of *child pornography* and to restricting child access to *inappropriate material*, but there have as yet been no reports of systematic technical filtering. There is, however, a body of laws, especially with regard to the activities of *journalists*, that is fairly restrictive. In a number of states, in response to drug trafficking and cartel activities,[27] there is widespread *self-censorship*, with many journalists preferring not to put their lives at risk and thus simply electing not to pursue dangerous information that may come to their attention. In Cuba, on the other hand, those few who manage to gain access to the web are constantly monitored and risk persecution at the first manifestation of dissent. Despite Cuba's recent declaration of Internet as a fundamental right for the Cuban people,[28] connections to the web require government authorization and are closely supervised by the Cuban M*inistry of Computer Technology and Communications*.

A recent essay by Kitzberger's analyzed the media activism of Latin America's *leftist governments*, with some topical remarks (Kitzberger 2010). The author describes the impact of ideology on Latin American government practices and policies regarding media and journalistic institutions, and discusses media regulation

[25] See the ONI *Regional Overview* concerning Latin America at http://opennet.net/research/regions/la. Accessed 24 November 2011.

[26] See the ONI *Country Profile* regarding Cuba at http://opennet.net/research/profiles/cuba. Accessed 23 November 2011. See, also, Sect. 6.2.2.

[27] See an interesting news (AFP 2012) concerning the web presence of cartels and the possibility to use it against them with hacktivism actions. " Mexico drug cartels […] have increasingly turned to the Internet to improve their communications, avoid detection, and recruit members, but officials say that reliance could be used in the fight against. […] Groups like the Zetas - a brutal gang of former hitmen - have also been using the web not just to help their operations, but to terrify their enemies and normal Mexican citizens with videos of executions, images of victims after torture and killing, and to hunt down critics who denounce violence online. An expert in military intelligence said those same methods could be used to obtain information on the gangs, notably to locate offenders using tracking methods that search through photos and messages from cellular phones. Press freedom groups have condemned growing attacks and killings of people who use social networks to share information in violent areas of Mexico, where traditional media no longer dare to report on relentless drug-related violence" (AFP 2012).

[28] See, *inter alia*, the article by Symmes regarding this issue (Symmes 1998). The journalist remarks that " […] the government of aging dictator Fidel Castro declared access to the Internet a 'fundamental right' of the Cuban people, and then made it impossible for ordinary Cubans to buy a computer" (Symmes 1998).

policies on the part of the recent leftist governments in Argentina, Bolivia, Brazil, Chile, Ecuador, Uruguay, and Venezuela. An interesting point concerns Internet grassroot activities (emphasis mine):

> At the grassroots level and on the Internet a myriad of discussion forums, blogs, web sites, community media, and publishing enterprises, all carrying discourses *critical* of mainstream media, emerged establishing a sort of *counter-information trench war*. These base-level initiatives aimed at questioning media *credibility* are linked to governments in different ways. In some cases, the link is limited to informal alliances with preexisting autonomous groups. Where governments are based on strong party organizations, as in Brazil and Uruguay, the grassroots activities tend to be embedded in the latter. In other cases, most notably Venezuela, the state plays a major role in shaping such decentralized initiatives. (Kitzberger 2010: 10).

In North Africa and the Middle East[29] there have been constant and extensive investments in information technology and developmental infrastructure. This is contrasted, however, by the fact that this area is, according to *OpenNet Initiative* studies on the region, one of the most *heavily censored* in the world. Countless cyber-dissidents and bloggers have been arrested in many of the region's nations. A single critical remark of the government of the monarchy, or a discussion of religious topics may be grounds for immediate imprisonment, and numerous laws have been passed to prevent the exposure of corruption or electoral fraud. When activist organizations draw up lists and classifications of the nations that are most repressive of blogger rights and activities, Egypt,[30] Syria,[31] Tunisia[32] and Saudi Arabia[33] regularly hold top positions. In these countries all possible techniques, from specific legislation, filters and blocks to threats and arrests, are used to monitor and control the flow of information. A large portion of censorship activities in this region takes place under the wide umbrella of laws controlling *the press*, which, in many countries, are considered applicable to online sources as well. Pervasive monitoring of the Internet activities takes place in Internet cafés (in many cases state-controlled) where video surveillance cameras are routinely installed. Almost all these cafés are monitored by dedicated servers that register all activities. Additionally, in a number of nations users are required to present identification before using Internet café computers. Content filtering is directed principally at *political* and *religious* matters, and site blocking and filtering activities intensify considerably during election periods in order to veil certain facts and to impede the diffusion of dissenting voices or anti-government

[29] See the ONI *Regional Overview* regarding North Africa and Middle East at http://opennet.net/research/regions/mena. Accessed 14 November 2011.

[30] See the ONI *Country Profile* concerning Egypt at http://opennet.net/research/profiles/egypt. Accessed 24 November 2011. See, also, Sect. 6.3.1.

[31] See the ONI *Country Profile* concerning Syria at http://opennet.net/research/profiles/syria. Accessed 24 November 2011. See, also, Sect. 6.2.5.

[32] See the ONI *Country Profile* regarding Tunisia at http://opennet.net/research/profiles/tunisia. Accessed 24 November 2011. See, also, Sect. 6.3.2.

[33] See the ONI *Country Profile* regarding Saudi Arabia at http://opennet.net/research/profiles/saudi-arabia. Accessed 24 November 2011. See, also, Sect. 6.2.4.

propaganda. Overall, in this area, technology investments are proceeding in two very clear directions: (i) technology for increased *development*, and (ii) technology for increased *control* of Internet use and access.

In many countries of sub-Saharan Africa,[34] where the diffusion of Internet is still at very initial phases, there is a strong history of *media abuse* and of *restrictions* on *freedom of the press*. In Ethiopia, for example, there are reports[35] of covert technical content filtering, although the volume of web users throughout the region is, for evident reasons, still quite low. In this Country, Ethiopia's only ISP, state-owned Ethio-Telecom, installed a system for blocking access to the Tor network.

A recent, interesting essay by Pelsinger discusses how *Web 2.0* is changing, and challenging, the *Truth and Reconciliation Commission of Liberia* (TRCL)[36] activities (Pelsinger 2010). Through the use of emerging technologies, notes the author, Liberia has empowered wide swathes of individuals to tell their stories in *previously unimaginable ways* (Pelsinger 2010: 731), and this fascinating report analyzes whether the very same social ethos that drives popular Internet sites and viral trends can be applied in the *human rights context*. Pelsinger's conclusions are that:

> Web 2.0 is one of several types of technologies that enable ubiquitous participation. Herein lies a key component of Liberia's Truth Commission: in a world increasingly affected by Web 2.0, and with the field of transitional justice growing more technology orientated, truth projects that encourage ubiquitous participation through Web 2.0 technology can do a better job of achieving their goals. They can task the citizenry with some responsibility for collaborating in the transitional justice process. […] bottom-up truth telling allows 'voices from below to be heard and heeded'. […] In the case of the LTRC, top-down and bottom-up initiatives existed simultaneously; the mandate and administration originated with the Liberian government, while Web 2.0 offered a bottom-up network of Liberian participants (Pelsinger 2010: 734).

In 2011 the *Electronic Frontier Foundation* (EFF) announced (and criticized) the intention of the South African parliament to pass a bill known as *Protection of Information Bill*, protecting government officials from *scrutiny* while preventing the public from accessing important information.[37] The bill, explains EFF, would challenge Article 32 of the South African Constitution,[38] which guarantees citizens the right of access to "any information held by the state" as well as "any information

[34] See ONI *Regional Overview* regarding Sub-Saharan Africa at http://opennet.net/research/regions/ssafrica. Accessed 24 November 2011.

[35] See ONI *Country Profile* regarding Ethiopia at http://opennet.net/research/profiles/ethiopia. Accessed 24 November 2011.

[36] See the official web site of the Commission at http://trcofliberia.org/. Accessed 23 November 2011.

[37] See the EFF announcement at https://www.eff.org/deeplinks/2011/11/south-african-bill-poses-grave-threat-press-freedom. Accessed 24 November 2011.

[38] The text of Article 32 of the South African Constitution is: "Access to information. Everyone has the right of access to any information held by the state; and any information that is held by another person and that is required for the exercise or protection of any rights. National legislation must be enacted to give effect to this right, and may provide for reasonable measures to alleviate the administrative and financial burden on the state".

that is held by another person and that is required for the exercise or protection of any rights", and furthermore decrees that "national legislation must be enacted to give effect to this right, and may provide for reasonable measures to alleviate the administrative and financial burden on the state." This bill, remarks EFF, would give the government virtually *unlimited authority* to classify as *secret* any information they wish; they are not required to give any explanation, and the process is not overseen by a court. According to EFF's experts, this bill would have *three* main damaging effects:

1. *punishment (also) for citizens and companies*. The law, EFF notes, institutes harsh punishments on *not only government officials* who *leak* this information, but also *private citizens* and *companies*, like bloggers, newspapers and television stations, who decide to publish the information;
2. *impossible proof*. The burden would be placed on journalists to have information declassified, but given the nature of classified information, the bill will effectively make *proving* that such information is in the "public interest" inherently impossible;
3. *no exceptions at all*. No *public interest exception* exists for journalists who publish classified information not authorized for release, meaning a journalist could potentially be thrown in jail for decades for publishing evidence of crimes that would normally send government officials to jail.

In the United States of America and Canada,[39] although active censorship activities may not be readily apparent (especially when compared to Asia, or Africa), according to ONI there are often attempts to *over-regulate* the Internet, or *special programs* for institutions such North American public libraries and universities, essentially mandating the use of *content filtering programs*. In the United States, the most well known cases involving legislative attempts at censorship have been motivated not only by the desire to protect minors, but also by purported national security and copyright protection concerns, computer security and protection from information warfare and cyber-war attacks. A final point, however, should be remembered: given the technological means available to the United States of America and the technical progress which characterizes this country, it is probable that it simply may not be possible to fully identify all current monitoring and surveillance activities. This is also (or, perhaps, especially) true of global covert monitoring practices, projects similar to *Echelon* and other secret, classified activities carried out by the NSA and other agencies.

In Canada, in 2008, Moon drafted a very interesting and complete report, addressed to the *Canadian Human Rights Commission*,[40] concerning Article 13[41] of

[39] See the ONI *Regional Overview* regarding United States of America and Canada at http://opennet.net/research/regions/united-states-and-canada. Accessed 24 November 2011.

[40] See the official web site of the Commission at http://www.chrc-ccdp.ca/default-eng.aspx. Accessed 14 November 2011.

[41] The text of Article 13, regarding *hate messages*, is the following (emphasis mine): " (1) It is a discriminatory practice for a person or a group of persons acting in concert to *communicate telephonically* or to cause to be so communicated, repeatedly, in whole or in part by means of the facilities of a telecommunication undertaking within the legislative authority of Parliament, any

the *Canadian Human Rights Act*[42] and the regulation of *hate speech* on the Internet (Moon 2008). The scope was to consider, and to make recommendations, concerning the most appropriate mechanisms to *address hate messages on the Internet*. The scholar takes the position that the censorship of hate speech should be *limited* to speech that explicitly or implicitly threatens, justifies or advocates violence against the members of an identifiable group (Moon 2008: 42). Moons's conclusions are evident (emphasis mine):

> The use of censorship by the government should be *confined to a narrow category of extreme expression* – that which threatens, advocates or justifies violence against the members of an identifiable group, even if the violence that is supported or threatened is not imminent. The failure to ban the extreme or radical edge of discriminatory expression carries too many risks, particularly when it circulates within the racist subculture that subsists on the Internet. Less extreme forms of discriminatory expression, although harmful, cannot simply be censored out of public discourse. Any attempt to exclude from public discourse speech that stereotypes or defames the members of an identifiable group would require *extraordinary intervention by the state and would dramatically compromise the public commitment to freedom of expression*. Because these less extreme forms of discriminatory expression are so commonplace, it is impossible to establish clear and effective rules for their identification and exclusion. But because they are so pervasive, it is also vital that they be *addressed* or *confronted*. We must develop *ways other than censorship* to respond to expression that stereotypes and defames the members of an identifiable group and to hold institutions such as the media *accountable* when they engage in these forms of discriminatory expression (Moon 2008: 1).

In 2011, concerning Canada, EFF reported[43] the draft of several *online spy legislative proposals* that threatened long held civil liberties and privacy rights. The *Online Spying Bills* (C-50, C-51 and C-52[44]), collectively called the "lawful access" bills, are essentially, EFF explains, a *backdoor* for law enforcement to easily access

---

matter that is likely to *expose a person or persons to hatred or contempt* by reason of the fact that that person or those persons are identifiable on the basis of a prohibited ground of discrimination. (2) For greater certainty, subsection (1) applies in respect of a matter that is communicated *by means of a computer or a group of interconnected or related computers*, including the Internet, or any similar means of communication, but does not apply in respect of a matter that is communicated in whole or in part by means of the facilities of a broadcasting undertaking. (3) For the purposes of this section, no owner or operator of a telecommunication undertaking communicates or causes to be communicated any matter described in subsection (1) by reason only that the facilities of a telecommunication undertaking owned or operated by that person are used by other persons for the transmission of that matter".

[42] See the full text of the *Act* at http://laws-lois.justice.gc.ca/eng/acts/h-6/. Accessed 14 November 2011.

[43] See the announcement at https://www.eff.org/deeplinks/2011/11/northern-exposure-unmasking-online-spying-canada. Accessed 23 November 2011.

[44] As Cavoukian remarks (Cavoukian 2011), these bills would regulate three important points: (i) *Bill C-50* would make it easier for the police to obtain judicial approval of *multiple intercept* and *tracking* warrants and production orders, to access and track e-communications, (ii) *Bill C-51* would give the police new powers to obtain *court orders for remote live tracking*, as well as suspicion-based orders requiring telecommunication service providers and other companies to *preserve* and *turn over* data of interest to the police, and (iii) *Bill C-52* would require telecommunication service providers to build and maintain *intercept capability* into their networks for use by law enforcement, and gives the police warrantless power to access subscriber information.

personal information, and include new police powers that would allow Canadian authorities easy access to Canadians' online activities, including the power to force Internet service providers to hand over private customer data without a warrant. Adding insult to injury, the legislation will also pave the way to gag orders that would prevent online service providers from notifying subscribers that their private data has been disclosed–a move that would make it impossible for users to seek legal recourse for privacy violations.

6.1.2 Techniques and Tools Commonly Used to Censor

In practice, we well see in the following pages, Internet censorship and restriction, as mentioned above, may be achieved though a wide range of available strategies. ONI studies testify that the first one is *technical blocking*, and there are several techniques utilized to block access to forbidden internet sites: *IP blocking, DNS tampering* and *URL blocking using a proxy*.

These techniques are often utilized to block access to *specific*, pre-defined web pages, suspect dominions and IP addresses (and even entire groups of IP addresses), and are implemented when physical control over the targeted site, or direct jurisdiction, are beyond the reach of authorities.

An even more advanced method of technical blocking is known as *keyword blocking*, which blocks access to web sites based on the words found in URLs or blocks searches involving certain blacklisted terms.

The second commonly used censorship technique is the removal of "forbidden" results from search engines.

In a number of instances, companies providing Internet search services have cooperated with governments to omit, from the results obtained from searches conducted from within the country's borders, sites considered illegal or, otherwise, undesirable.

This makes it more difficult (but not impossible) to find those sites, or to connect to the pages they contain, especially if the search engine user is not an expert.

The third common censorship strategy is known as *take down*, used when those who desire to regulate a certain behavior, and have targeted a determined site, have direct access to and full jurisdiction over web content hosts.

In this case, the strategy adopted is that of simply demanding, if necessary following a trial or other legal action, the removal of web sites containing content considered inappropriate.

As mentioned above,[45] often even a "simple" cease-and-desist letter sent by an attorney claiming damages (for example: to an Internet service provider), is more than enough to intimidate and sufficiently persuasive to obtain the removal of all the contested material. When authorities have direct control of systems for domain

[45] See Sect. 3.9.2.

name management and of the servers hosting a site, they may also operate directly on the name of the site and demand that it be de-registered in order to effectively render it invisible to users' browsers.

The fourth method is quite subtle and even more insidious. It consists, in fact, of inducing subjects to *self-censor* their own activities. A widespread strategy is to create an atmosphere of terror and threat sufficient to induce individuals to avoid publishing content in any way critical of the regime. Threats employed range from the risk of legal action to strict forum regulation, from arrest or threat of incarceration, to simply making citizens aware that all Internet activity is closely monitored.

Internet filtering can occur at any or all of four network nodes (or control points). First of all, national state-directed content filtering schemes and blocking technologies may be implemented directly on the Internet backbone, the "central nerve" of Internet connections, thus conditioning Internet access throughout an entire country. A second level is that of Internet Service Providers (ISPs): government authorities oblige ISPs to install determined filtering programs or to adhere to specific surveillance schemes.

A third, also quite commonly used level, targets connections originating in determined institutions, such as companies, public libraries, universities, and cybercafés. Increased control over specific types of institutions is common in many countries (for example, the United States, where, for a number of years, public libraries have been pressured by the government to implement filtering software, and Tunisia, with its government run, and controlled, cybercafés). Clearly, institutional-level filtering may be used to achieve two quite different aims; either, often in order to meet internal objectives, impeding unauthorized use of technological resources in a productive reality (such as disallowing use of gaming sites on company computers during working hours) or, at the behest of the government, to control Internet users. The fourth and final node at which filtering may be implemented is found, as might be expected, on home or individual computers, which may contain specifically installed filtering software providing true local, real-time censorship restricting the computer's ability to access certain sites.

Nearly all filtering technologies, however, not only harm fundamental liberties, but are also often flawed. These techniques, which can significantly affect individual freedoms, are prone to two principal weaknesses: *underblocking* and *overblocking*. *Underblocking* is the failure of filtering systems, despite their significant complexity, to fully block the millions of sites, many small and not highly visible, that contain prohibited content, or to block other computer-based media such as e-mail, forums, mailings lists, news groups or social networks. It is fairly common for these systems to block only the most visible sites, allowing users to freely consult everything else. *Overblocking*, on the other hand, is the blocking of legitimate content which the system was not intended to block. Blacklists, for example, contain, in addition to expressly designated restricted sites, sites which have been targeted as the result of automated searches generated by the filter software and which may have no relation at all with forbidden content or may be included simply for having the same server or provider or having a similar IP address.

There are two further important points to consider as well. First of all, it is clear, given the simple mass of currently existing web content, that nations and authorities must nearly always rely on private software providers, especially in those cases in which ISPs systems are utilized. This signifies that, in many states, the control of citizens' freedoms (and of their online communication) is nearly always in the hands of private, commercial entities. The second point is that filtration systems are generally *proprietary*, and there is thus *no transparency* whatsoever with regard to how they operate, what criteria are used for *labeling* and *restricting* targeted sites, or to whether they also perform additional, undocumented, activities.

6.2 An Analysis of Several Countries with Critical Human Rights Issues

6.2.1 Burma: Internet and Human Rights in a Particular Technological, Political and Legal Framework

6.2.1.1 Internet Connection in Burma: A Political and Technical Overview

Burma, officially *The Republic of the Union of Myanmar*, has had a military government since 1989, and has developed a wide range of means to maintain *strict control* over all media[46] and to limit the distribution of any content considered even potentially damaging to the regime's political principles and its reputation. The rigid, repressive approach adopted in the last two decades by the military Junta toward those who express opinions contrary to the regime not only violates the freedoms of speech and of expression of its citizens, but is also, unfortunately, only one aspect of an overall political strategy that systematically violates the human rights of the country's citizens. Due to the objectively difficult situation with regard to human rights in Myanmar, the country is under *close observation* by numerous international organizations, and on diverse occasions numerous nations have applied sanctions, in the form of trade embargos and the suspension of aid, as a consequence of the anti-democratic behavior of the government.

Internet has been available in Myanmar only since 2000,[47] and the particularly limited characteristics of Internet access in this country have lead to its pejorative

[46] See the interesting work of Nordahl concerning contemporary exile journalism, including a case study of *The Democratic Voice of Burma* (Nordahl 2009).

[47] See another interesting analysis, by Dacanay, regarding Internet usage by Burmese ethnic migrants, especially *marginalized women* in Mae Sod and Internet divide problems (Dacanay 2010). The author notes (emphasis mine): "The Internet has ostensibly liberating effects on these women, but this paper proposes that there is more to the feeling of being free in the virtual world. There is currently a "project" of *affirming*, *claiming*, and *molding* traditional ethnic identities through the use of Internet. The paper imagines this as revolutionizing the discursive mode of resistance and rebellion by these marginalized women against the military regime in Burma.

nickname, the MWW (the *Myanmar Wide Web)*. As a result of the government's stronghold over all aspects of the country's Internet access and content, Myanmar has been defined by the *Committee to Protect Journalists* as the worst country in the world for bloggers[48] and *Amnesty International* has long included it in its blacklist of *Internet Enemies*.[49]

The instruments utilized by the government range from blocking access to Internet with infrastructural and legal barriers and pervasive content monitoring and filtering to coercive measures and heavy sanctions for all transgressors. All of this occurs in an overall climate of constant surveillance and fear which work together to foster the most efficient instrument for repression and control: *self-censorship*.

Internet access in Burma is limited, deliberately, by a body of laws regulating this medium, by the lack of infrastructure and slow connection speeds, but also due to the general poverty of its population and to high costs of telecommunication services in general.

In a country in which it is estimated that 32% of the population lives below the poverty line and where 70% of monthly salaries go toward food purchases, the price of an Internet connection is prohibitive; this results in Myanmar having one of the world's lowest Internet penetration rates. Currently less than 1% of the country's population uses Internet. Data regarding telephone access recounts a similar tale: in 2009 there were only 0.1 mobile telephone accounts per 100 inhabitants and 1.62 landlines. The cost of a SIM card (available in the country since 2009) is also quite high, and permitted only upon presentation of valid identification, a copy of which must be conserved by the retailer. Additionally, in order to obtain a private Internet connection, clients must first procure a government license, and in order to secure this license individuals must be able to demonstrate that they have never been involved in unauthorized political activities. Due to these restrictions, the country's approximately 2,000 broadband subscriptions are used primarily by government functionaries and businesses, while the principal mode of Internet access for the majority of web users in Myanmar is the Internet cafés, which are also subject to a series of precise rules and regulations. Officially, there are 433 "Public Access Centers" (PACs); many of these are state-run but the number is increasing and there

---

Using their agentic qualities, the women transform their social scripts as "marginalized" and "displaced" into "*empowered*" women who are informed, educated, and aware of their human rights". The scholar remarks also that (emphasis mine): "Studies have shown how the Internet has provided *liberating effects* especially on individuals in conflict-situated areas […] Indeed, what became clear from our data was the importance of the Internet in providing a *space or refuge* to migrant women who are displaced because of the political situation in Burma and who now live in a quasi-hospitable and quasi hostile and restricting environment in Thai towns by the border. While the movements of their bodies are restricted *their minds are free* to explore and travel to far away places through the Internet. The Internet becomes a window to the outside world, so to speak" (Dacanay 2010: 1).

[48] The *Report* may be found at the address http://www.cpj.org/reports/2009/04/10-worst-countries-to-be-a-blogger.php. Accessed 23 October 2010.

[49] The blacklist can be viewed at http://12mars.rsf.org/i/Internet_Enemies.pdf. Accessed 23 October 2010.

are a great many Internet cafés operated without any license at all (over 1,000 in the Rangoon area alone). PACs are prohibited from installing software to circumvent government restrictions, but some allow clients to utilize their own laptops.

As if the severe limits to web were not sufficient, the government also controls the country's infrastructure and, consequently, all flow of information. The nation's only two ISPs, *Myanmar Teleport* (MMT) and *Myanmar Post and Telecommunication* (MPT), both belong to the state. This has permitted the government to "shut-down" the Internet on several occasions. During the cited widely-followed protests led by Buddhist monks in 2007 (which will be further discussed below), in order to avoid transmission abroad of images, video and news of the protests and of the harsh military reactions they engendered, the government literally "turned off" the telecommunications network, with a complete Internet shut-down lasting nearly 2 weeks. The same occurred in 2008 in the aftermath of hurricane *Nargis*. In this case, the interruption of service not only sought to avoid images of the population's suffering due to the natural calamity, but also to elude any criticism of the government's aid efforts. In addition to programmed Internet shut-downs, slowdowns in connection speed are not infrequent, particularly during critical periods such as elections.[50]

Complete control over the country's infrastructure also provides the government with nearly complete control over all web content. According to recent *OpenNet Initiative* tests,[51] both state-run ISPs, MMT and MPT, blocked (during the ONI observation period) the same number of circumvention tools, including *Proxify*, *Proxyweb*, *Guardster* and *Proxyweb.net*. Periodically, *Gmail* and *GoogleTalk* are also blocked, while *Skype* and other VoIP services are generally prohibited. The same report demonstrates that search engines and their additional services (such as *Google Groups*, *Picasa*, *Google Docs*, *Google News*, *Google Translate*) are generally accessible, while free e-mail services, such as *Yahoo! Mail*, *Gmail*, *Hushmail*

[50] For a detailed history of political, legal and social events in Burma, and their connection with the Internet and the United States government, see the essay by Danitz and Strobel about *networking dissent*, the promotion of democracy in Burma and limitations that activist NGOs face when confronting resolute authoritarians (Danitz and Strobel 2001). The authors note that (emphasis mine): "The case of Burma raises intriguing questions about the effect of modern computer communications on the *balance of power* between citizens and elected officials, and among local, national, and international power structures and, ultimately, their effect on the conduct of diplomacy in the 21st century. Geographically dispersed but knitted together by the Internet, Burmese and non-Burmese activists from the United States as well as from Europe and Australia joined a long standing effort to bring democracy to Burma (a small, and to many, obscure Southeast Asian nation). Their global campaign raised *constitutional and national policy questions* in the United States, as a state government and local councils passed foreign policy legislation without consulting Washington. […] We offer evidence that the Internet was crucially influential in enabling civil society actors to *force the passage* of a series of laws regarding business and political dealings with Burma. The Internet was also used to sway international public opinion and pique the interest of more traditional news media. In particular, we find that, among its many and still unfolding uses, the Internet - by its very nature - lends itself as a potent tool for advocates organizing for action on international issues" (Danitz and Strobel 2001: 130–131).

[51] See the ONI Country Profile concerning Burma at http://opennet.net/countries/burma. Accessed 23 October 2011.

and *mail2web*, are often filtered. One of the two ISPs also blocks *Flickr*, *YouTube* and *Blogspot*, while international and national newspaper sites are filtered by both service providers.

However, in Myanmar the majority of censorship activities is directed toward web sites defending human rights and democracy, from the sites of international organizations such as *Amnesty International* and the *United Nations* to sites focusing on human rights in Myanmar itself.[52] The government actively seeks to block any keywords considered "dangerous", including "Burma", "drugs", "military government", "democracy", "student movement", "8888" (date of the student movement giving rise to the revolt of August 8, 1988) and "human rights".

Monitoring is pervasive, and the punishments meted out to transgressors are severe. Myanmar has received international criticism for the arbitrary application of numerous incriminatory laws, some resulting in sentences of over 65 years in prison.

Government attempts to repress the Internet and the rights of its citizens are hardly consistent with its declarations to the effect that it desires to extend web access within the country, and to improve available services and infrastructure, while at the same time it continues to maintain its rigid stance and to adopt increasingly repressing measures.

6.2.1.2 The Legal Framework in Burma

The Constitution of Myanmar, approved by referendum only in 2008, sadly appears to be little more than a *façade*. The rights it grants, in fact, are in no way respected in practice.

Especially worthy of note is Article 354 of the Constitution,[53] which guarantees the *freedom of expression*, but at the same time establishes strict limits as to the exercise of this right. In particular, generic references to activities that are not illegal, to peace in the community, public order and morality are clearly little more than instruments to repress, limit and censure the Burmese population.

Quite different are the laws limiting the liberty of expression, both those precedent and those subsequent to the ratification of the country's Constitution. First and foremost of these is the Penal Code,[54] containing numerous sections routinely used

[52] See, for example, http://burmacampaign.org.uk. Accessed 23 October 2011.

[53] The text of Article 354 of the Constitution reads as follows: "Every citizen shall be at liberty in the exercise of the following rights, if not contrary to the laws, enacted for Union security, prevalence of law and order, community peace and tranquility or public order and morality: (a) to express and publish freely their convictions and opinions; (b) to assemble peacefully without arms and holding procession; (c) to form associations and organizations; (d) to develop their language, literature, culture they cherish, religion they profess, and customs without prejudice to the relations between one national race and another or among national races and to other faiths". English text of the 2008 Constitution can be found at http://www.burmalibrary.org/docs5/Myanmar_Constitution-2008-en.pdf. Accessed 23 October 2011.

[54] The Burmese Penal Code can be viewed at the address http://www.blc-burma.org/html/Myanmar%20Penal%20Code/mpc.html. Accessed 23 October 2011.

against political activists, bloggers, journalists, dissidents or any member of the population who dares to manifest dissent with the regime. Section 130 (b)[55] in fact, establishes the crime of offence to state agencies, and section 295 (a)[56] that of insult to religion, while section 505 (b)[57] establishes the crimes of jeopardizing the public order and of incitement to the commission of a crime.

Moreover, there is abundant legislation utilized in Myanmar to repress the freedom of expression.

Censorship of all news is made possible by the application of a law dating back to 1962, known as the "Printers and Publishers Registration Act",[58] requiring authorization for any written or printed material prior to its publication.

Precedent to the above law is the *Emergency Provisions Act* (1950), limiting freedom of speech for any individual attempting to distribute false information about the government. This law is still in force. In 1996 two laws, both widely applied today, were passed. The first, called the *Computer Science Development Law*[59] punishes anyone possessing a television, satellite decoder or video recorder without express authorization of the *Ministry of Communications, Posts and*

[55] See the text of Section 130 (b): "Whoever, by words either spoken or intended to be read, or by signs or by visible representations, publishes anything tending to degrade, revile or to expose to hatred or contempt any Foreign State, Head of State, Ambassador or other dignitary of a Foreign State, with intent to disturb peaceful and friendly relationship between the Union of Burma and that Foreign State, shall be punished with imprisonment of either description for a term which may extend to three years, or with fine, or with both".

[56] See the text of Section 295 (a): "Whoever, with deliberate and malicious intention of outraging the religious feelings of any class of persons by words, either [through] spoken or written [means], or by visible representations, insults or attempts to insult the religion or the religious beliefs of that class, shall be punished with imprisonment of either description for a term which may extend to two years, or with fine, or with both".

[57] See the text of Section 505: "Whoever makes, publishes or circulates any statement, rumour or report, (a) with intent to cause, or which is likely to cause, any officer, soldier, sailor or airman, in the Army, Navy or Air Force to mutiny or otherwise disregard or fail in his duty as such; or (b) with intent to cause, or which is likely to cause, fear or alarm to the public or to any section of the public whereby any person may be induced to commit an offence against the State or against the public tranquility; or (c) with intent to incite, or which is likely to incite, any class or community of persons to commit any offence against any other class or community, shall be punished with imprisonment which may extend to two years, or with fine, or with both".

[58] See the text of Article 6: "(1) Registration of printers and publishers. As enacted by other means in this law, according to paragraph Three, all printers and publishers having made and signed an agreement must apply to have their own business registered within the period of time specified according to the method of application designated by the appropriate registration official. (2) No-one may engage in either printing or publishing without a registration certificate issued in accordance with this law in compliance with the rules or requirements relating to the certificate". The text of the law is at the address http://www.ibiblio.org/obl/docs3/Printers_and_Publishers_Registation_Act.doc. Accessed 23 October 2011.

[59] See the text of the Law that can be found at the address http://www.mcpt.gov.mm/mcpt/myanmar-computer-science-development-law.htm. Accessed 23 October 2011. See, for example, Article 26: "(a) The Ministry of Communications, Posts and Telegraphs may, with the approval of the Council determine by notification the types of computer to be imported, kept in possession or utilize only with the prior sanction of the Ministry. (b) In determining the types of computer

Telegraph, and also sanctions anyone using these technologies to copy, distribute, sell, or exhibit video recordings without authorization from the state censorship board. Penalties for any violations are quite severe.

The other 1996 law is the *Television and Video Law*[60]; by Article 3, which describes the objectives of the law, its negative potentials are abundantly clear, given that it is so plainly open to arbitrary interpretation.[61] This law also establishes the obligation to obtain prior authorization in order to possess a television, a video recorder, or a satellite receiver.[62]

---

under sub-section (a), fax-modem card installed computer which can transmit or receive data shall be primarily targeted. (c) In determining the types of computer under sub-section (a), it shall not apply to computers that are used only as aids in teaching, office work or business"; Article 27: "A person desirous of importing, keeping in possession or utilizing the type of computer prescribed in sub-section (a) of section 26 shall apply to the Ministry of Communications, Posts and Telegraphs in accordance with the stipulations to obtain prior sanction"; Article 28: "A person desirous of setting up a computer network or connecting a link inside the computer network shall apply to the Ministry of Communications, Posts and Telegraphs in accordance with the stipulations to obtain prior sanction"; Article 29: "The Ministry of Communications, Posts and Telegraphs may, after scrutinizing the applications submitted under section 27 or section 28 in accordance with the stipulations, grant prior sanction or refuse to grant prior sanction"; and Article 30: "A person desirous of keeping in possession or utilizing the type of computer prescribed under sub-section (a) of section 26, shall comply with the orders and directives issued from time to time by the Ministry of Communications, Posts and Telegraphs with respect to issuance of licence, prescribing the term of licence, licence fee and licence conditions". Article 31 and 32 establish several sanctions: "31. Whoever imports or keeps in possession or utilizes any type of computer prescribed under sub-section (a) of section 26, without the prior sanction of Ministry of Communications, Posts and Telegraphs shall, on conviction be punished with imprisonment for a term which may extend from a minimum of 7 years to a maximum of 15 years and may also be liable to a fine"; and Article 32: " Whoever sets up a computer network or connects a link inside the computer network, without the prior sanction of the Ministry of Communications, Posts and Telegraphs shall, on conviction be punished with imprisonment for a term which may extend from a minimum of 7 years to a maximum of 15 years and may also be liable to a fine".

[60] The full text of the law can be found at http://www.blc-burma.org/html/myanmar%20law/lr_e_ml96_08.html. Accessed 23 October 2011.

[61] See the text of Article 3: "The objectives of this law are as follows: (a) to modernize and uplift the standard of video business; (b) to cause the emergence of video tapes which will be beneficial for the all-round development of the State and the preservation of Manmar cultural heritage; (c) to cause emergence of video tapes which contribute towards national solidarity and dynamism of patriotic spirit; (d) to prohibit and ban decadent video tapes which undermine Myanmar culture and Myanmar tradition; (e) to control and prevent malpractices which are caused trough video business".

[62] See the text of Chapter III: "Chapter III - Licence for Possession - 4. Any person who holds and uses a television set or a video cassette recorder shall apply for licence for possession, in accordance with the stipulations to the relevant post office within 30 days from the date of receipt of the same. 5. (a) The applicant shall pay the fee payable out of the following fees in accordance with the stipulations to the relevant post office: (i) fee of the licence for possession; (ii) overdue fee; (iii) extension fee; (b) On receipt the prescribed fee the relevant post office shall issue the licence for possession to the applicant. 6. Upon the expiry of the tenure of the licence for possession, a person desirous of extending such tenure shall have the extension effected by paying to prescribed fee to the relevant post office. 7. The Ministry of Communications, Posts and Telegraphs shall determine the tenure and fee of the licence for possession, overdue fee and extension fee. 8. Any person who is desirous of possessing any satellite television receiver shall comply with the order and directives relating to import, possession, use, transfer, sale, issuance of licence, determination of licence fee and licence conditions, issued from time to time by the Ministry of Communications, Posts and Telegraphs".

The same laws law creates, among other agencies and government bodies, the "Video Censor Board", which has the function, among others, to control imported video tapes and examine them.

This law, as well, provides for harsh prison sentences in the event of any violations.[63]

The *Telecommunications and Post Ministry* intervened to further regulate this issue with Notification no. 8/2002, known as the *Wide Area Network Order* (2002), and in 2004 yet another law, called the *Electronic Transaction Law* of 2004, after having established definitions, scope of application and aims, and after having created the *Central Body of Electronic Transactions* and provided for the detailed regulation, highly susceptible to arbitrary application, of all electronic commerce, establishes a series of truly draconian penalties for all prohibited behavior.[64]

---

[63] The text of Chapter IX – Offences and Penalties is: "31. Whoever with the exception of a Government department and government organization operates the television transmission business without the premission of the Government shall, on conviction, be punished with imprisonment for a term which may extend to 5 years or with fine. In addition, the property which relate directly to the offence shall also be confiscated. 32. Whoever commits one of the following acts shall, on conviction, be punished with imprisonment for a term which may extend to 3 years or with tine which may extend to kyats 100,000 or with both. In addition, the property which relate directly to the offence shall also be confiscated: (a) operating video business for commercial purpose without a video business licence; (b) copying, distributing, hiring or exhibiting the video tape that has no video censor certificate and small-sized video censor certificate with the permitted serial number with the exception of cases exempted under this Law; (c) copying, distributing, hiring or exhibiting the video tape without abiding by the directive of the Video Censor Board to make excision, amend or erase; (d) exhibiting to the public the video tape imported or brought from a foreign country without video censor certificate; (e) exhibiting to the public the video tape imported or brought from a foreign country and which is permitted only for the family show. 33. Whoever commits one of the following acts shall, on conviction, be punished with imprisonment for a term which may extend to 3 years or with fine which may extend to kyats 100,000 or with both:- (a) distributing, hiring or exhibiting the copied television programme transmitted by the government department or government organization, for commercial purpose; (b) copying, distributing, hiring or exhibiting for commercial purpose a video tape which has already obtained video censor certificate, without permission of the licence holder of video production business or video tape distribution business. 34. If any video business licence holder operates video business other than the kind for which he holds licence he shall, on conviction, be punished with imprisonment for a term which may extend to 1 year or with fine which may extend to kyats 100,000 or with both. In addition, the property which relate directly to the offence shall also be confiscated. 35. If any video business licence holder transfers his video business licence to another person to operate he shall, on conviction, be punished with imprisonment for a term which may extend to 6 months or with fine which may extend to kyats 50,000 or with both. 36. Whoever fails to abide by an order or directive issued by the Ministry of Information or Video Censor Board or the Video Business Supervisory Central Committee under this Law shall, on conviction, be punished with imprisonment for a term which may extend to 6 months or with fine which may extend to kyats 50,000 or with both".

[64] See the text: "33. Whoever commits any of the following acts by using electronic transactions technology shall, on conviction be punished with imprisonment for a term which may extend from a minimum of 7 years to a maximum of 15 years and may also be liable to a fine: (a) doing any act detrimental to the security of the State or prevalence of law and order or community peace and tranquillity or national solidarity or national economy or national culture. (b) receiving or sending and distributing any information relating to secrets of the security of the State or prevalence of law and order or community peace and tranquillity or national solidarity or national economy or

The government of Myanmar would not appear to have any intention whatsoever of altering its repressive orientation, not even following the 2010 elections.

In April 2010, an official from the government's *Cyber Crime Department* reportedly warned that the state would impose harsh punishment for any online activities related to politics.

If this were not enough to establish the truly repressive line of the country's legislation, in September 2010 the *Union Election Commission* (UEC), in admitting 37 political parties to participate in the election, issued a series of highly restrictive regulations creating significant limitations to all freedom of expression, with the result that the elections were denounced by the entire international community for the antidemocratic fashion in which they were conducted, including several instances of arbitrary detention of members of the opposition.

Lastly, in May 2011, the government further enforced control over the country's Internet cafés, prohibiting the use of CD-ROMs, USB memory sticks, floppy disks and all other external memory devices.

Only a few months before, the Burmese junta had declared all VoIP systems illegal.

Thus, the Burmese legal framework is, to say the very least, highly problematic.

The combined application of the laws and regulations described above has resulted in the imprisonment of countless Burmese bloggers, activists, politicians, comedians, authors and directors, some of whom have received truly absurd sentences of over 65 years of imprisonment. The international community has often

---

national culture. 34. Whoever commits any of the following acts shall, on conviction be punished with imprisonment for a term which may extend to 5 years or with fine or with both: (a) sending, hacking, modifying, altering, destroying, stealing, or causing loss and damage to the electronic record, electronic data message, or the whole or part of the computer programme dishonestly; (b) intercepting of any communication within the computer network, using or giving access to any person of any fact in any communication without permission of the originator and the addressee; (c) communicating to any other person directly or indirectly with a security number, password or electronic signature of any person without permission or consent of such person; (d) creating, modifying or altering of information or distributing of information created, modified or altered by electronic technology to be detrimental to the interest of or to lower the dignity of any organization or any person. 35. Any certification authority or any of his officer or employee who violates any of the prohibitions contained in the order issued by the Control Board shall, on conviction be punished with imprisonment for a term which may extend to 3 years or with fine or with both. 36. Whoever violates any of the prohibitions contained in the rules, notifications and orders issued under this Law shall, on convition be punished with imprisonment for a term which may extend to 1 year or with fine or with both. 37. Whoever commits any of the following acts shall, on conviction be punished with imprisonment for a term which may extend to 1 year or with fine or with both:- (a) knowingly misrepresents to the certification authority his identity or authorisation in applying for a certificate or in submitting for suspension or cancellation of a certificate; (b) obstructing or impeding or assaulting the Central Body and body or person assigned duty by it or the Control Board and body or person assigned duty by it which performs the functions and duties in accordance with this Law or failing to comply with the demand to perform in accordance with this Law. 38. Whoever attempts to commit any offence of this Law or conspires amounting to an offence or abets the commission of an offence shall be punished with the punishment provided for such offence in this Law".

come to the defense of human rights in Myanmar, but the government has yet to enact any concrete measures.[65]

To this must be added the fact that thanks, in large part, to the country's legal framework, today in Myanmar there are approximately 2,200 political prisoners and prisoners of conscience.

Individuals accused of having committed crimes against the government are not guaranteed the right to defense and are not permitted to call witnesses in their defense. They are often coerced to confession by means of torture, the accused are incarcerated while awaiting their trials, and this period of detention is not detracted from their sentences, in clear violation of constitutional rights and procedural rules. Trials take place behind closed doors, and often witnesses for the defense, when present, are themselves accused and incarcerated.

Prisons and work camps offer no medical assistance to detainees, who are subjected to generally inhuman conditions.

6.2.1.3 Censorship Circumvention and the Role of Technology in the *Saffron Revolution*

In a context so generally threatening to the rights of its citizens, the hope for increased freedom of expression is common to nearly all Burmese. In 2010 alone, blogging activity within the country increased by 25%, as compared to the previous year, and in the first 3 months of 2011, 13% of all cyber attacks worldwide originated in Myanmar. The owners of Internet cafés assist citizens in evading controls, permitting the use of private laptops, or even, putting their own freedom at risk, providing VoIP and VPN services located in Canada or the United States. Digital resistance activities thereby consist both of the use of blogging platforms as tools for liberty, and of the creative use of new technologies for the purpose of evading state control and repression.

In 2007, observers of digital resistance witnessed the most important popular revolt against the military regime in Burma since the student uprisings of 8/8/1988.

Jacobi highlights very well the digital differences between the two events (emphasis mine):

> The events of 8/8/88 may be etched in the memory of Burmese people […], but there is little *photographic evidence*. In contrast, in 2007 there was documentation *from the beginning*, in the form of digital images taken by cameras and camera phones. As the protests grew, new technology played a pivotal role. Access to mobile technology in particular represented a sea change in how information was transmitted and what it meant for the people involved, because mobiles connected protesters to each other and to the outside

[65] See the study by Chowdhury on the role of Internet in Burma's *Saffron Revolution* (Chowdhury 2008). According to the author (emphasis mine): "The 2007 Saffron Revolution in Burma was in many ways an *unprecedented event in the intersection between politics and technology* […] and […] the event marks a rare instance in which a government leveraged control of nationalized ISPs to entirely *black out* Internet access to prevent images and information about the protests from reaching the outside world" (Chowdhury 2008: 2).

> world. In a closed society where people fear the consequences of speaking openly with a neighbor, new technology allowed for *new kinds of mobilization*. Information was broadcast to organizations operating freely in exile, including in Thailand, India and Bangladesh. Information was then transmitted back inside by trusted contacts, allowing many people to take part. […] Throughout the unrest, protesters, including monks and laypeople, used mobiles to coordinate the logistics of the protests, communicate breaking news to Burmese living in exile and international news organizations, and to document them through mobile images and mobile video that were either uploaded via the Internet and shared with international news sources or smuggled out—on discs and flashdrives— through underground networks to neighboring countries. All this was coordinated and executed with the added restriction that international text messaging didn't exist for Burmese mobile users (Jacobi 2011: 145).

Due to stringent government control of the media, it is generally very difficult to obtain news and other information on the situation in Burma, especially during times of protest. This revolution, however, was different. The movement now known as the *Saffron Revolution*,[66] named for the color of the robes of the Buddhist monks who lead the uprising, came to international attention only as a result of the Burmese bloggers and activists who inundated the web with photographs, videos and news of the revolt. Individuals throughout the country became citizen journalists, taking photos and shooting videos that were subsequently uploaded to the web from countless Internet cafés. The protest first arose as a consequence of the government's announcement of the end of state subsidies for gasoline, diesel and natural gas. This resulted in a significant and unexpected rise in the prices of gasoline and diesel, which only worsened an economic situation for the citizens of Burma that had already reached critical levels. At the beginning, a small number of monks took to

[66] See, *inter alia*, a study by Mottaz regarding new media in closed societies and the role of digital technologies in Burma's *Saffron Revolution* (Mottaz 2010). The author notes (emphasis mine): "The 2007 uprising is a *unique example* of a technology driven protest in a highly authoritarian state. […] Despite government restrictions, citizen journalists and digital activists have found *innovative ways* to circumvent restrictions. Many install foreign-hosted proxy servers, allowing users to access Gmail and other blocked sites. Hyper-encrypted e-mail services are also used to evade government censorship of e-mail content. According to experts, these circumvention techniques have been very successful and the junta has been unable to control their use. The outbreak of the Saffron Revolution demonstrates this […] Access to digital technologies in 2007 enabled activists to *stay organized and informed*. Mobile phones played a *crucial role* in keeping protestors connected by reducing communication times from weeks to mere seconds. Mobile phones played an indispensable role in the pro-democracy campaign. They permitted monks and activists to coordinate their protests to generate the most pressure on the regime. Mobile phones also allowed activists to stay *in contact* during the protests and warn each other about military movements […] Burmese bloggers also played a critical role in the uprising by providing citizens with information about the protests […] Due to the lack of broad Internet access in Burma, Internet initiatives found the most success when coupled with traditional forms of mass communication, particularly radio and satellite television. During the uprising, news updates from Internet blog sites were quickly transferred into television and radio broadcasts […] These technologies also allowed activists to *connect with the international community*. Pictures, video footage, and commentary reached international news agencies via the Internet within hours. The speed at which information about Burma's democracy protests reached the outside world had a significant impact on the movement because the international community was able to quickly react to this information and support protestors by putting pressure on the Burmese regime" (Mottaz 2010: 3, 5).

the streets in peaceful protest against this measure, but within only a matter of days the number of protesters grew to over 50,000. The military response the unarmed crowds was nothing short of brutal, and images of the violent retaliation made front pages around the world.

The government sought to contain the situation with mass arrests, torture and killings. However, despite the efforts of the government to control the media, images and news of the uprisings continued to make their way out of the country; for this reason, on September 29, 2007, in a desperate attempt to close off the domestic situation from international eyes, the regime completely shut down all Internet connections and all telephone lines within the country, neatly cutting Myanmar off from all outside communication. This situation lasted for nearly 2 weeks. The government response to the uncontrolled flood of news on the revolt demonstrates how much it desperately desired to maintain total control over the media, and how difficult this is to do in the era of new technologies, which render the task of controlling the flow of information over the Internet far more difficult as compared to the control of traditional media.

Jacobi provides valuable insight on the situation, and on the role of mobile phones in Burma as well (emphasis mine):

> The Southeast Asian nation lags far behind its neighbors (including Bangladesh, China, India & Thailand) in mobile penetration, yet the advent of mobile phones has had far-reaching impact on the country's volatile political situation, economy as well as *censorship* and *surveillance practices*. Much of this is shaped by the 2 month period of August to September 2007, when mobile phones played a critical role in protests that challenged the military regime. Armed with camera phones and limited Internet access, Buddhists monks coordinated the largest protests witnessed in years, *broadcasting* the story to the outside world. These tools proved so threatening that the Burmese government responded by shutting off all Internet and mobile phone communications for 5 days. Although a technological blackout was the government's initial response, in time the commercial need for mobile phones has trumped the political concerns, and today the country is witnessing increased access to mobile phones as well as service, at a rate unimagined even a few years before (Jacobi 2011: 141).

It remains to be seen whether in the case of Burma, despite the enormous potential of new technologies and their fundamental role in supporting democracy and human rights, protest,[67] even that conducted and witnessed through the use of new digital technologies, will be sufficient to bring about any measure of concrete change.

[67] See the study by Thiha on the role of the local bloggers and of the Burmese blogosphere during the Saffron revolution (Thiha 2010). The author notes (emphasis mine): "As Burmese blogosphere is developed through Saffron Revolution, the blogs are still in revolutionist nature. It is require developing into cyberspace for political discussion. The relationship between political blogosphere and non-political blogosphere is still weak. Although we cannot identify the locations of the bloggers we can assume *most of the bloggers are from outside* Myanmar by interpreting the numbers of posts. Empowering and encouraging citizens inside Myanmar is required to increase participation and discussions in both cyberspace and blogospheres to improve equal participation. Burmese political blogosphere can be regard as the space that can *criticize* the government actions however; it is still not possible to interpret their political ideology as posts are only intended to *against the regime*. It is also too early to conclude that Burmese political blogosphere is representing *the voice of citizens* inside Myanmar as participations from inside Myanmar are low" (Thiha 2010: 8).

6.2.2 *Cuba: Internet Control, User Restrictions, Legal and Regulatory Frameworks, Blogosphere, Digital Dissidents and Civil Society*

6.2.2.1 Internet in Cuba: An Introduction

Cuba, with a population, in 2011, of approximately 11,451,650 inhabitants and a very low number of Internet users, approximately 1,604,000, has been defined, since the placement of the very first cables, by the presence of two *parallel networks* that coexist on the island: the Internet *per se*, international in both origin and outlook (although, as we shall see, filtered, controlled and limited in content) and a closed, national network, even more heavily controlled by the Cuban government, containing a system for e-mail (addresses ending in ".cu") used above all in academic and public/governmental environments, and fairly limited content, including an encyclopedia and several government managed news and information sites.[68]

Aside from the coexistence of these two networks, the overall technological, legal and political situation in Cuba not only merits closer analysis simply due to its singularity and distinctiveness, but its very uniqueness also renders it extremely useful for the researcher.

The report of *Amnesty International* on the restrictions of the freedom of expression in Cuba states (emphasis mine):

> The current legal framework and the way in which it is enforced by the authorities *seriously limits freedom of expression*. A range of laws are used to curb the legitimate expression of *opinion* and *dissent*. People continue to face unfounded criminal prosecution, as well as harassment and intimidation by state security and police officials, for expressing and distributing information or opinions critical of the government. Unlawful *restrictions on freedom of expression* are underpinned by other restrictions on human rights, such as the *rights to freedom of association*, of *peaceful assembly* and of *movement*. Arbitrary detention, interrogations and warnings at police stations, and other forms of temporary arrests are frequently used by the authorities to intimidate individuals critical of the prevailing state system. The cumulative effect of such practices has been to create a climate of fear in Cuban society and inhibit the development of freedom of expression. The *judiciary* is neither independent nor impartial and allows criminal proceedings to be brought against those critical of the government as a mechanism to prevent, deter or punish them *for expressing dissenting views*. The complicity of the state judicial system in prosecuting government critics, often in summary trials that fail to meet international fair trial standards, has a *profound chilling effect* on freedom of expression, association and peaceful assembly. Political dissidents and other critics of the government were in many cases harassed and intimidated by organized groups of government supporters; these may include local members of the communist party and members of pro-government mass organizations, in particular

[68] For an overview of the technological framework see the *Cuba Study Group* article regarding how to empower the cuban people through access to technology (CSG 2010): "There are several obstacles to the development of information technology in Cuba, including the impact of economic sanctions by the United States. However, the primary reasons for Cuba's underdevelopment in ICT stem from the Cuban government's own policies, which aim to prioritize political control over economic development and information infrastructure" (CSG 2010: 220).

> Committees for the Defence of the Revolution and Rapid Response Brigades. There are reports of combined activities between government supporters, state officials and law enforcement agencies to harass dissidents (Amnesty 2010: 2).

Researchers in this field, in particular, agree that there are three principal defining factors for the current environment in Cuba:

1. the embargo,[69]
2. the widespread poverty that plagues the country, and
3. the stringent control over nearly every aspect of life exerted by the government and the ruling (and only) party.

The first factor, the embargo, has, in addition to other well-known aspects pertaining to politics and to the country's international relations, lead to a series of highly practical technological difficulties. Cuba is an island; an island, in order to enjoy rapid Internet access, must be cabled, that is, at least a minimum number of cables must be placed in order to provide for the physical connection to the Internet, located on the mainland. Lacking this physical, cabled connection, satellite and mobile telephone connections constitute the only other alternative, but these are quite slow and extremely expensive. Now, the waters surrounding Cuba are crisscrossed with diverse data cables, but those originating in Florida, a mere 90 miles away, do not touch it due to the embargo (and also due to a certain political mistrust of American technology). In 2011, however, there arose the possibility of connecting to the Venezuelan cable system, by means of a 1,000 mile long cable, financed by Venezuela (thanks to a loan from China), which would provide Internet cabling for Jamaica as well. If this project is eventually realized, it will be the first "real" efficient connection to the Internet ever available in Cuba, and will certainly transform the current technological panorama.

The embargo has had profound effects not only with respect to the island's cabling (or lack thereof) but also to all technology locally available on the island. The Cuban government bans the importation of most electronic devices to the island (especially satellite receivers), and, despite a certain softening on the part of the United States of America with regard to the possibility of United States of America telecommunications companies to work around the embargo to make technological

[69] See, *inter alia*, the article by Boas regarding Internet in Cuba and the United States of America policy (Boas 2000) and the *Internet dilemma*. The author remarks (emphasis mine): "Authoritarian leaders in the information age are confronted with an unmistakable dilemma. On the one hand, the Internet and associated information and communication technologies offer *enormous economic potential* for developing countries, and the increasingly interconnected global economy *thrives on openness of information*. On the other hand, the information revolution poses *new challenges* for regimes that rely on *centralized* political control" (Boas 2000: 57). The scholar notes, also, that (emphasis mine): "Networks of dissidents and reform-minded NGOs have shown that they can use new technological tools *to place pressure* on their governments, but their information-empowered activism is limited by their access to technology, a factor over which regimes can choose to retain full control" (Boas 2000: 66). Also interesting is the study by Fitzgerald concerning *blacklisting* and *secondary boycotts* (Fitzgerald 1998), and the essay by Bowman on *export controls* in the digital era (Bowman 2004).

investments on the island, the technological environment in Cuba is still obsolete, available lines are few and inefficient, and computer illiteracy is rampant. Cuba, in fact, was the very last Latin American country to finally establish a connection to the Internet. Only in March 2008 did Raoul Castro remove some of the restrictions on technology, allowing the sale of cellular telephones and computers to civilians.

The second defining factor, the island's pervasive poverty, creates enormous limits to the ability of Cuban citizens to access the Internet. E-mail is the most widely utilized tool. The ban on household connections has led to the necessity of using public Internet facilities, including those located in the island's hotels and resorts, which however tend to be quite expensive and generally affordable only for tourists and foreign visitors and functionaries, in addition to being widely monitored and pervasively controlled, thus facilitating retaliation for any unauthorized use. Thus the extremely high costs of technology in Cuba have rendered Internet a tool for the island's élite. Due to the poverty of its citizens, mobile phones and computers are nearly impossible to obtain.

The third factor, no less important, is the fear on the part of the Cuban government and its desire to *control the flow of information* over all the nation's media, including the Internet.[70] The country's single telecommunications provider, ETESCA, facilitates the centralization of this control, together with a rigid legal framework and a state-run filtering system that blocks pornographic sites and those containing content that is in any way contrary to the dominant political doctrine. ETESCA also controls the Internet access of the island's civilian citizens, who, in order to connect must be "approved" by this Agency and by a commission connected to the *Committee for Defense of the Revolution Act*.

It must additionally be noted that, as a consequence of the activities of a number of famous Cuban bloggers who have received international attention, the local government has restricted Internet access even further, allowing its use only by researchers, academics and government workers who are permitted to have an Internet account, but with enormous limitations on what foreign content they may access. Cuban citizens are allowed to have e-mail accounts, which they access from local post offices, but they may not access the Internet. Tourists to the island may access Internet from their hotels, but with restrictions, and since 2009 Cuban civilians may no longer use hotel Internet services.

Approximately 14% of the Cuban population has access to Internet; access is thus extremely limited and there is an increasing tendency on the part of the government to further develop its already nearly total control of the flow of information

[70] See the study by Hoffmann regarding how the Internet can change state-society relations in an authoritarian regime such as Cuba (Hoffmann 2011). The scholar writes that (emphasis mine): "A precondition for civil society activism to evolve is *some degree of public sphere* in which it can 'breathe'. The state monopoly on mass media, as exercised by the Cuban state, has been a particuary thorough form of authoritarian control over the national public sphere. The comparative empirical analysis of civil society dynamics in the 1990s and in the 2000s has shown the notable impact of the digital, web-based media on the contours of the public sphere and has also demonstrated that this, in turn, impacts the *activities*, *conception* and *organizational forms* of societal actors" (Hoffmann 2011: 25).

within the country. In addition, posting content considered by the state to be "counter-revolutionary" may result in sentences of up to 20 years of imprisonment, and any unauthorized access carries a prison sentence of up to 5 years.

This third factor has understandably resulted in a climate of pervasive self-censorship. Very often, in fact, it is Cubans themselves who are afraid of approaching this medium, avoiding use of it altogether and controlling their own actions for fear of government retaliation.

Finally, the phenomenon of *reverse filtering* originating the United States deserves mention here; due again to the atmosphere of political and commercial conflict between the two nations, a number of filtering systems based in the United States of America recognize Cuban IPs and block access to external information sources. This renders even more difficult any flow of information from the island.

The scholar Venegas provides a vivid description of this singular landscape (emphasis mine):

> Digital media seeps into the everyday life of Cubans just as currents of *political transition breathe* greater dimension to individual expression and visions for the future. The generation of Cubans joining the digital era are grandchildren of the revolution, without firsthand memories of its victories and accomplishments. Their lot has been defined by the hardship of extreme times. This generation and its aspirations, complaints, and desires is changing and intensifying the nature of opposition to the government through fresh forms of expression. The call for new approaches to reform, expressed by citizens and the Cuban-based opposition, is informed by different roots of *discontent* than those underlying the demands of hardline exiles. The clamor from inside Cuba is infused with rebellious racial politics, plainly evident in Cuban popular culture, in response to an *immediate sense of exclusion*. New avatars of citizens appear on new media channels, relating personal stories and experiences through blogs, electronic discussions, journals, artworks, and local community organizations. A new social imagination has begun to shape the future of Cuba, taking it beyond earlier rhetoric even where that rhetoric is digitized (Venegas 2010: 184).

6.2.2.2 The Cuban Legal Framework

The Cuban laws, regulations and ordinances limiting both Internet and traditional media are numerous, and found on diverse levels of the island's legal and legislative systems. The ambiguity of many of these norms has resulted in the regulation of the new medium, Internet, being easily placed under the umbrella of other, fairly unrelated laws and norms. This ambiguity of the laws, and their references to apparently general principles, has led to a legal situation in Cuba that is widely known to be repressive.

The first source of such laws, the Constitution, would certainly appear to establish a number of rights; in reality, however, the passages in which they appear are in fact used *against* dissidents. In particular, all these rights are subordinated to the wellbeing of the communist State, the revolution, and the ideology of the State.

A preliminary analysis, in order not of the sequence of the articles as they appear but of the concepts they contain, might begin with Article 62 of the Cuban Constitution, which establishes, for example, that none of the rights granted to the nation's citizens may be exercised in a manner contrary to the laws and the

Constitution of the country or contrary to the existence or the objectives of the socialist state.

This, in practice, concretely limits the exercise of the freedom of speech and the rights of association and of peaceful assembly. In Cuba, debate is generally permitted only when arguments presented by both sides support and the regime are in line with the objectives of the Cuban revolution. This is also true of the Constitution.

However, many Cubans seek *uncensored spaces* which are not subject to censorship.

The Constitution expressly subordinates the right to the freedom of the speech to the objectives of the socialist society, in Article 53, and the right to cultural expression is guaranteed only is the expression of the same is not contrary to the revolution, pursuant to Article 39.

The *Cuban Criminal Code* establishes numerous offences which can be applied to dissenters and to anyone daring to criticize the government: *propaganda enemiga, desacato, rebelión, actos contra la seguridad del estado, clandestinidad de impresos, difusión de noticias falsas, estado peligroso predelictivo, asociaciones, reuniones y manifestaciones ilícitats, resistencia, difamación, calumnia.*

All of the charges cited above have been used to restrict the freedom of speech in Cuba.

In particular, the *Cuban Criminal Code* establishes five different typologies:

1. security measures and "dangerous disposition";
2. crimes compromising state security;
3. crimes against the administration and the judiciary;
4. crimes against public order, and
5. crimes against honor.

Regarding *"Dangerous disposition" and security measures*, the Criminal Code separates security measures in two categories, pre-criminal security measures, set forth in Articles 78–84, which are applied in order the prevent the commission of an offense, and post-criminal security measures, detailed in Articles 85–90, which are applicable only after an individual accused of a crime has been tried.

The security measures are established and applied by a Court when an individual demonstrates that he or she is dangerous.

Key to the application of such security measures is "dangerous disposition", which in Article 72 of the Criminal Code is defined as "the special inclination of an individual to commit crimes as demonstrated by behavior which clearly is contradictory with the norms of socialist morality". Thus an individual demonstrating "dangerous disposition" might also exhibit anti-social behavior, habitually violating the rules of co-existence with acts of violence and or the rights of others, or might disturb the public order or live as a parasite exploiting the lives of others or practice vices which are socially unacceptable. Socially dangerous, rules of socialist co-existence, socialist legality.

Concerning *crimes compromising state security* (Article 91), these provisions may also be used against dissidents. Many of the 75 dissidents involved in the

crackdown of March 2003 were tried and convicted on the basis of Article 91 of the Criminal Code.

Crimes against the administration and the judiciary are set forth from Article 129 to Article 173. These are used to sanction any criticism of the government and the administration. Article 144, for example, establishes the offence of *desacato* sanctioning any lack of respect for state officials, and includes all forms of offense or disrespect, whether oral or written, of a public official. This article is often used to *silence dissidents* who criticize the activities of individual members of the administration. Article 143, on the other hand, sanctions resistance to a public official and is generally applied when an individual resists arrest. Due to the significant ambiguity of this article, it is also frequently applied to cases of non-violent resistance.

Finally, the concept of *public order* as set forth in Article 200 is extremely wide-reaching, and thus easily used to impede all demonstrations, to stifle dissent and to restrict the freedom of speech.

There are five principal offences relative to violations of public order: (i) insult to national symbols (Article 203), used against anyone insulting the national flag or other symbols; (ii) defamation of national institutions, organizations, heroes and martyrs (Article 204); (iii) conspiracy to commit a crime (Article 207), meeting in a group of three or more individuals with the intention of committing an illegal act or of interrupting a public gathering or event; (iv) illicit association, meetings and demonstrations (Articles 208 and 209), that punishes those who belong to associations not legally registered or who attend illicit meetings; (v) clandestine press (Article 210).

Last, but not least, *defamation* is classically used against honor, and is set forth in Article 318.

Very important as well, is Law 88 of February 1999. The *Cuban National Assembly* approved this harsh legislation, effectively criminalizing any direct or indirect support of the United States of America and US policy, as established by the Helms-Burton Act. It is called *Law 88 for the Protection of National Independence and of the Cuban Economy*, but the country's dissidents call it the *Gag Law*. It establishes prison sentences of up to 20 years in prison for any individual found guilty of *passing information* to the US government or even of searching for classified information. The provisions of this law are utilized to restrict the legitimate exercise of the right the free speech. Article 7.1, in particular, provides for prison sentences of up to 5 years for anyone working with foreign radio or television stations, printed publications or any other foreign media. It was widely used in the crackdown against journalists. In addition, leaving Cuba without express authorization is considered an offense to public order; this is clearly a restriction of the right to the freedom of movement, and prevents many activists and bloggers from ever leaving the country.

The Criminal Code and Law 88 both provide for prison sentences for those found guilty of activities considered to even potential risks, which disturb the peace, which are found to be counter-revolutionary, or in some way detrimental to the economy or to the country's independence. Law 209 of 1996 establishes that the Internet may not be used in violation of the moral principles of Cuban society

or of the laws of the state, and that email messages may not pose any threats to national security. "*Access from the Republic of Cuba to global information networks*" regulates Internet access according to Cuba's interests. Priority is given to legal entities and to institutions of great national importance which could benefit from having a connection. It is not designed for individuals, but rather for institutions and offices. In 2007, Resolution 127 concerning web security prohibited the distribution over public networks of any information contrary to social interests, norms of good behavior, personal integrity or national security. ISPs in Cuba are thus required to install systems in order to check for "detect" software programs and other similar programs, and to immediately report any such findings to the appropriate authorities.

Resolution 56/1999 establishes that material intended for publication or distribution over the Internet must first be approved by the *National Registry of Serial Publications*. Resolution 92/2003 prohibits e-mail providers and ISPs from to allowing access to individuals who have not been previously approved by the government, and allows activation of solely national, and not international, chat forums. Those who do not follow these directives may have their operating licenses suspended or revoked. Resolution 179/2008 requires all ISPs to censure material found to be in conflict with state security or contrary to social, ethical or moral interests. ETESCA is authorized to take all necessary action to prevent access to sites containing undesirable content. Resolution 179/2008 requires all ISPs to censure material found to threaten state integrity or contrary to social, ethical or moral interests. ISPs must also maintain records detailing all traffic data for the period of at least 1 year. Customs regulations prohibit the entry into Cuba of satellite telephones or GPS devices or satellite connections.

In April 2003, nearly 100 journalists and political dissidents who had been arrested the previous month were speedily tried, and handed sentences ranging from 6 to 28 years in prison. *Amnesty International* identified all the accused as "prisoners of conscience" and demanded their immediate release. All had been accused either on the basis of Article 91 of the Cuban Penal Code or pursuant to Law 88. Article 91 establishes prison sentences of up to 20 years, or even the death penalty for anyone committing, in the interest of a foreign state, acts intended to damage the independence or territorial integrity of the Cuban state. Resolution 180/2003 establishes that Internet services may be utilized only when their costs are calculated in a far more expensive method based on US dollars, in order to prevent any unauthorized use of such services. The telephone company actively seeks out and attempts to impede all access to the Internet from traditional telephone lines.

6.2.2.3 Restrictions to the Freedom of Expression in Cuba and the Human Rights Situation

Rather than using sophisticated blocking and filtering technologies, as is the practice in nations such as China and Tunisia, Cuban authorities may rely on the near absence of communication technologies on the island, and the exorbitantly high

costs of any available technology, to limit access to any external information sources. Additionally, sluggish connection speeds render access difficult to all but the simplest and most basic sites. The majority of sites belonging to dissidents, in the United States specifically and outside Cuba generally, are blocked, as they are deemed counter-revolutionary. It is also a crime to work with any international media not directly working for the government, a fact that has generated not only significant self-censorship but also renders anonymity even more important for anyone desiring to speak out. Dissidents and activists also make use of the *sneakernet*, physically passing any sensitive information on USB memory sticks rather than risking e-mail or web-based exchanges.

The principle that individuals may be imprisoned for exercising their rights to free speech is one of the fundaments of international law, recognized in many nations, but not in Cuba. Nearly 60 activists, at the present writing, are imprisoned solely for having expressed their dissent. Internet has provided additional means to evade government controls and censorship, but the state's media monopoly and the ban on possession of mass media instruments for private citizens, established by the Constitution, and similar restrictions applied to the Internet in Cuba only increase the power of the state and of the ruling party to control and monitor the island's inhabitants. Freedom of expression is progressively weakened with the justifications of national security, independence, and national sovereignty.

The three key elements developed by Cuban authorities to implement ever wider-reaching restrictions and control are:

1. the government's virtual monopoly over all media, from television and radio to print works and ISPs,
2. the government requirement that all journalists join the national association of journalists, totally controlled by the Cuban Communist Party, and
3. a number of provisions and articles in both the Constitution and the Criminal Code that are so vague as to allow police officials and magistrates free reign to restrict the freedom of expression of Cuba's citizens. Article 53 of the Constitution acknowledges the freedom of the press, but expressly prohibits private citizens from possessing any mass media devices. It is the objective of the socialist society to create explicit restrictions. There are independent news agencies, but they cannot be legally recognized. No criticism whatsoever is permitted of either government actions or the state of the national economy.

Access to the Internet is regulated by the *Law of the Security of Information*, which specifically prohibits access to the Internet from private habitations. Wideband connections are limited, essentially available only via satellite, at extremely high costs. Since 2009, the Cuban Postal Services has been authorized to host Internet cafés. Many Cuban blogs are not accessible from within Cuba due to pervasive filtering.

Journalists must mandatorily join the *Unión de Periodistas Cubanos* (UPEC) in order to carry out their work, and this association in its by-laws recognizes the

Cuban Communist Party as its "most important driving force". Obligatory membership in an association is a patent violation of Article 20 of the Universal Declaration of Human Rights. In this case, this requirement clearly exists solely for the purposes of exercising political control. Only journalists whose work is in line with the government and who do not dare to criticize it may belong to the association, independent journalists are excluded and therefore may not, for example, receive official authorization to follow events.

Cason clearly describes the human rights situation in Cuba (emphasis mine):

> We refuse to allow the Government of Cuba to define the boundaries of our contacts with Cuban citizens whom we see as individuals simply attempting to exercise rights due unto them as established in, and agreed to by the Government of Cuba in the Universal Declaration of Human Rights. As recently as March 20th at this year's session of the UN Human Rights Commission, Cuban Foreign Minister Perez Roque, described the Universal Declaration of Human Rights – and I quote him here – 'as a landmark in the collective aspiration to build a world of freedom, justice and peace'. […] On the very day that the foreign minister made these remarks, Cuban State Security agents *were rounding up dozens of human rights activists* and - not incidentally - seizing thousands of copies of the Universal Declaration of Human Rights. Despite the foreign minister's recognition of the importance of the Declaration, the Government of Cuba has previously cited it as a *subversive document*. This juxtaposition of *rhetoric* and *reality* is the very mechanism Fidel Castro has used for four decades to distract international attention from what truly ails Cuba: Its fundamental *disregard* for the rights of its own citizens. For too long, Fidel Castro has obscured Cuba's problems in the veil of national sovereignty, and his fractious relationship with the United States. The substantial and continued international reaction to Castro's latest crackdown demonstrates that this chicanery no longer fools anyone […] However, while Cubans welcome international recognition of their plight under the present government, it is the Cuban legal system itself that provides the strongest indictment of the regime - a regime based on maintaining political control at any cost to its citizens. This is not U.S. rhetoric; it is Cuban reality as defined by the Government itself in the Cuban Penal Code which begins: This code has as its objectives to protect society, people and the social, economic and political order, and the State regime.... To promote strict observance by the citizens of their rights and duties.... To contribute to the formation in all citizens of respect for socialist legality and compliance with the duties and the correct observation of the norms of socialist life. The Penal Code then codifies laws against 'dangerousness', 'contempt for authority',.... 'illegal assembly',.... 'illegal printing', and creates broad categories of crime such as 'enemy propaganda' and 'propagation of false news'. I highly recommend that students of Cuban affairs study both the Penal Code and the 1976 Cuban Constitution. These are the best tools for understanding the role of the Cuban state, and the liberties it takes in arbitrarily defining offenses against it. We in the U.S. are hard-wired to live in an open society; the authors of these documents clearly mistrust their own people and are hard-wired against a free society (Cason 2003: 54, 55).

6.2.2.4 Public Sphere, Blogosphere, Dissidence and the Civil Society in Cuba

Concerning the important role of blogs in Cuba, Yoani Sánchez is Cuba's most famous blogger, who has created a worldwide following for herself by simply commenting on daily life on the island in a forthright fashion that national and even

international media never have.[71] The relationship with the independent press and with dissenters has been difficult since Fidel Castro came to power. With dozens of independent journalist in prison, the states seems to be conducting a sort of internal news embargo against its citizens. Cuba, in fact, is the nation with the highest per capita number of imprisoned journalists (Gómez 2008).

Cuban dissident bloggers have become internationally famous, and this has led the government to implement further restrictions to Internet access, in an attempt to silence these dissenting voices. The government seems to fear bloggers more than traditional activists, who are more easily controlled.

Technological tools create public space, and today in Cuba technology is going a long way in facilitating a sort of subterranean guerrilla war that may very well lead to a more widespread reaction. A first aspect involves opening toward culture and arguments that are not official, outside the sphere of the state. All of this is driven by a thirst for transparency and the desire to show the world what is occurring and allow the events and facts of an entire people to finally move beyond the borders of their state, to the eyes, minds and hearts of the rest of the world.

[71] For a brief overview of Yoani's activities, see the essay by Henken regarding the *emergent blogosphere* in Cuba (Henken 2011). The author remarks that: "Anyone who has read Generación Y over the past three and a half years will have noted Sanchez's great faith in the power of a wide and growing variety of information and communication technologies (ICT) - including blogs, Twitter, Facebook, You Tube, as well as internet-ready Flipcams and smart phones that can send SMS texts and e-mails and record voice, photos, and video. For her, these technologies have the potential to help "level the playing field" between authoritarian governments and marginalized citizens – whether they be Iranian voters, Chinese dissidents, or Cuban bloggers. She also clearly believes that such ventures into cyberspace can help these citizens begin to create more public space where they can exercise the full rights and responsibilities of true citizens". It is still too early to determine the depth of the impact of the Cuban blogging phenomenon. The fact that the government has blocked Cuba's most influential independent blog, Yoani Sánchez's Generación Y, now for more than 2 years, has repeatedly denied Sánchez permission to travel abroad, and has gradually augmented its media and physical attacks against her, all indicate that it is concerned about her growing influence. Her growing international profile and ability to sway global public opinion about the Cuban regime along with her increasingly audatious public activism for freedom of expression within the island make her simultaneously impossible to ignore and dangerous to repress. At the same time, given the extremely low level of Internet connectivity in Cuba and the fact that the government continues to control the totality of the island's mass media, we are still far away from any so-called "blogostroika," where the Internet and independent blogs can effectively challenge the state's monopoly on information. For their part, neither Sánchez nor the rapidly expanding group of independent cyber-activists who work alongside her, show the least indication of ceasing to provoke the regime by living as full citizens with all the rights and duties the term implies. Sánchez openly admits that what began for her as an individual project of personal catharsis has been transformed over time into a collaborative international media project that seeks to go beyond the constraints of cyberspace in order create more free and independent public space within the island for open debate about Cuba's many difficult challenges. Openly skeptical, Sánchez rejects "verbal violence," cynicism, personal attacks, and the disqualification of those who think differently – all unfortunate characteristics with deep roots in Cuban political culture and commonplace on both sides of the Straits of Florida. Her goal is to create a pluralistic, respectful, and serious civil dialogue in her beloved patria. She intends to accomplish this goal through the transparent exercise of her particular brand of citizen cyber-journalism (Henken 2011: 125).

Concerning the civil sphere and challenges to the regime, and their limits, Otero and O'Bryan observe (Otero and O'Bryan):

> Informal dissidence alone, therefore, is insufficient to accomplish a democratization of the regime. Given its widespread occurrence in Cuba, however, we can establish that Cuban civil society has reached the equivalent of Weigle and Butterfield's defensive stage of development, in which individuals and atomized groups try to protect themselves against the party-state. The Cuban state, of course, has so far weathered the systemic crisis of the Special Period better than the Eastern European cases-that is, it is still in power. The question then becomes whether civil society can advance, in its own fashion, to the second, emergent stage, in which independent social groups or movements act in a wider, state-sanctioned public sphere. The Cuban state has not yet allowed the creation of any autonomous public sphere; it has used either strict repression tactics (imprisonment, execution) or exile to drain the ranks of known activists […] Nevertheless, a number of organized groups and coalitions have emerged or resurfaced in Cuban civil society. With the rise of the Internet, however, dissident groups, like the Ladies in White, have found an international podium that does not depend on traditional media. Cubans have surpassed the challenge of getting their message to the Internet, but the question remains as to whether their message is reaching the nearly ten million Cubans on the Island who do not have regular, uncensored Internet access. While state-owned traditional media made total control of dissident messages relatively easy, the Internet now limits the state to partial control and only within the territorial boundaries of the country. New technology has created an outlet completely outside official channels for Cubans. As in other authoritarian regimes, the Internet promotes discourse, but it alone is not likely to produce widespread political change (Otero and O'Bryan 2002: 39).

In 2012 Yoani Sánchez formally filed a notice with the Interior Ministry demanding to know why she's not allowed to travel abroad. As Tamayo reports (Tamayo 2012):

> Sánchez said the notice filed Wednesday asks Interior Minister Abelardo Colomé Ibarra to explain why the ministry office that is in charge of exit permits never answered her Nov. 18, 2010 request for the reasons behind the refusals. Colomé Ibarra now has 60 days to respond to her complaint of "administrative silence," Sanchez said. If he doesn't, she will file a lawsuit against the minister seeking a court order that he must reply. "Of course, I know what's going to happen. But I want to maintain that innocence of having hope," Sánchez added, referring to the high probability that her complaints will go nowhere in a country where the courts faithfully follow the government line. Cubans who want to travel abroad require a government permit, known as a "White Card" and regularly denied to dissidents. It has turned down several Sánchez requests to travel abroad to receive prizes, attend conferences or for other reasons. She has repeatedly asked for an explanation at the Interior Ministry's Office for Immigration and Foreigners' Affairs, but received none. Her notice Wednesday elevated her question to the minister's office. "It's a step before a lawsuit," she told El Nuevo Herald by phone from Havana. "It is a legal, juridical opportunity in the hands of citizens, which allow an appeal against Cuban authorities when the authorities have not responded to a petition." Her notice was the latest in a handful of bold attempts by dissidents and others to use Cuba's legal system to challenge official actions. The courts have knocked down almost all the cases, including some filed against police. But the Cuban Juridical Association is still fighting a three-year-old case seeking the legal recognition of the Justice Ministry as a group of lawyers that provides legal advice on a nonprofit basis, usually to government critics. CJA chief Wilfredo Vallín, who also is advising Sánchez on her case, took the first step required to register the group in April 2009 by asking the Justice Ministry's Registry of Associations to certify that no other group had registered the same name. The registry never replied so the 1992 graduate of the University of Havana Law School elevated his request to Justice Minister María Esther Reus. When she didn't reply,

> he filed suit under Cuba's Law for Civil, Administrative and Labor Procedures. To his surprise, a three-judge panel first officially accepted Vallín's complaint, and then ordered Reus to appoint lawyers to defend her. Cuba's highest court, the Supreme Tribunal found a technical fault with one of his filings last year but allowed the case to continue and later ordered the minister to reply to Vallín's initial request. The Justice Ministry certified last June that no other group was registered with the same name or purpose as the CJA, but earlier this year it rejected the CJA's application for recognition on technical grounds. Vallín has vowed to appeal. Ministry officials had never officially recognized any dissident group, making them illegal and therefore subject to sanctions for the crime of "illegal association." Cuba's justice system argues that the role of the law is to promote stability and the development of a "socialist society." Dissidents put on trial are almost always convicted. Lawyers are required to work for the government or government-approved Collective Law Offices, where criminal defense attorneys can be hired. But lawyers who spend too much time defending dissidents are sometimes fired from the law offices (Tamayo 2012).

6.2.2.5 Ladies in White: Online Activism Against Repression

The activities of the *Ladies in White* (*Las Damas de Blanco*), an extremely well-organized group of Cuban activists that began as a response to the *Black Spring* (*La Primavera Negra*) of 2003, an out-and-out crackdown against nearly 100 of the nation's journalists and dissidents, all of whom were subsequently incarcerated. This group of courageous mothers, wives, sisters, daughters, cousins, neighbors and friends make use of both traditional and online methods of civil disobedience and their activities offer an excellent example of digital resistance activities in this country and of the consequent problems that may ensue.

These women protest against Fidel and Raul Castro's regime. They began in 2003 following the incarceration of numerous dissidents, many of them family members. On March 17 2010 one of their peaceful marches ended in violence when many of them were cruelly beaten and dragged away through the streets of Havana. Thanks to the Internet, the violence used by Cuban police officials against these women became public, thanks to a series of photos, videos and eye-witness reports posted on the web. Videos of the women being beaten while they held up pictures of their imprisoned loved ones began to circulate on *YouTube*. Despite the restrictions surrounding Internet access, countless Cuban citizens uploaded videos and photos to the web. What was fascinating was that when word of these protests eluded government control of the media in Cuba and were rendered public, they began to exert a certain degree of influence, so much so that after only a few months the government began to release the prisoners.

A digital camera was sufficient to bear witness to what had occurred. While in Cuba traditional media can no longer be depended upon to adequately divulge information, new technologies are increasingly used to overcome these failures.

As Del Riego and Rodriguez remark (emphasis mine):

> With the rise of the Internet, however, dissident groups, like the Ladies in White, have found an *international podium* that does not depend on traditional media. Cubans have surpassed the challenge of getting their message to the Internet, but the question remains as to whether their message is reaching the nearly ten million Cubans on the Island who do not have

> regular, uncensored Internet access. While state-owned traditional media made total control of dissident messages relatively easy, the Internet now limits the state to partial control and only within the territorial boundaries of the country. New technology has created an outlet completely outside official channels for Cubans. As in other authoritarian regimes, the Internet promotes discourse, but it alone is not likely to produce widespread political change. (Del Riego and Rodriguez 2011: 239).

6.2.2.6 Some Technical Issues: Censorship Circumvention and the Cuban Network

The cited[72] diplomatic document published by *WikiLeaks*, entitled *Surfing the Net in Havana*, describes well the attempts of an American diplomat and his wife to access the Internet on normal day. After finding numerous facilities either closed or out of service, they managed to access the Internet from a hotel terminal. *Where can one surf?* Using *Google Cuba* (google.cu) it was possible to access numerous official web sites, including USINT, his own head office, but also the sites of the US Department of State and the UN, international human rights and NGOs such as *Human Rights Watch* and *Amnesty International*; access was via satellite and therefore extremely slow. It was not possible to change the browser from *Google.cu* to *Google.com* or to any other Google site, nor was it possible to access any Cuban dissident group. The final consideration of the official was that the Cuban population utilizes nearly exclusively e-mail, and he closed by suggesting that Washington D.C. send aid in the form of instruments to evade filters and to facilitate internet navigation.

Despite the government's actions to limit access to the Internet within Cuba, and although they have a nearly complete monopoly over the media throughout the country, it has not been possible to completely block access, and Cubans continually seek to circumvent their government's restrictions. Passwords for Internet access may be purchased on the black market, foreign friends buy pre-paid cards, and new systems and tools that permit users to evade blocks and filters and to access forbidden sites are constantly being developed.

American mobile telephones do not work in Cuba because the US service providers do not provide roaming services there. However, any inexpensive unlocked telephone allowing GSM tri-band communication may be used with SIM cards that can now be bought in Cubacel offices.

Special permission may be obtained to use Internet, but Internet connections in Cuba are some of the most monitored and filtered in the world, with all e-mail communications carefully verified by the state apparatus.

Cuban civilians must utilize state access points, which are monitored using three different methods: (i) IP blocking, (ii) browsing history checking, and (iii) keyword filtering. At Internet cafés there are two types of connections, a national connection, consisting of little more than e-mail operated by the government and an international

[72] See Sect. 1.4.

connection, with access to the worldwide web, but most Cubans are limited to the national network, due, among other reasons, to the high costs involved.

The best way to bypass Cuban filters and Internet firewalls is to use a VPN service, located in the United States, to access unlimited sites and video streaming. Often the government limits and identifies sites based on the domain names, creating alternative names. Web proxies may thus be useful to access forbidden sites through a portal. Translating services are useful as well; if *Google Translator* is not blocked, a bit of creative thinking may allow the user to access translations of blocked sites.

Last, but not least, in 2011 Cuba sentenced Alan Gross, a United States citizen, to 15 years in prison for acts against the independence or territorial integrity of the Cuban state when he attempted to use communication media without authorization "in order to subvert the Cuban revolution". He was arrested at the Havana airport with computers that he was bringing onto the island. He worked with the *Development Alternatives Incorporated*, which was seeking to provide the island's Jewish population with instruments to connect via computer, via telephone and via satellite to the Internet.

6.2.3 South Korea: Digital Resistance Issues

South Korea occupies the southern portion of the Korean Peninsula. Unlike the northern portion of the peninsula, governed by a socialist dictatorship, since the 1990s South Korea has enjoyed a progressively democratic government with an expanding economy in which technology plays a key role.

Internet is widely available throughout the country, with user rates superior to 80%[73] of the population. Following years of heavy investment, South Korea's infrastructure is innovative and highly developed, featuring advanced wideband availability and over 114 ISPs. The country is, in other words, one of the *most connected* in the world, and even the government has acknowledged that Internet and user-generated content have acquired significant power over virtually all aspects of life.

The Constitution is South Korea's most important regulatory source, and reflects the modern democratic principles upon which the country is founded. Article 21[74] establishes *the freedom of speech*, bans censorship and underlines the importance of

[73] See http://www.internetworldstats.com/stats3.htm. Accessed 19 November 2011.

[74] The full text of Article 21 reads: "Article 21 [Speech, Press, Assembly, Association, Honor, Public Morals] (1) All citizens shall enjoy freedom of speech and the press, and freedom of assembly and association. (2) Licensing or censorship of speech and the press, and licensing of assembly and association shall not be recognized. (3) The standards of news service and broadcast facilities and matters necessary to ensure the functions of newspapers shall be determined by Act. (4) Neither speech nor the press shall violate the honor or rights of other persons nor undermine public morals or social ethics. Should speech or the press violate the honor or rights of other persons, claims may be made for the damage resulting therefrom".

a free press. The last paragraph, however, appears to directly contrast the preceding sections of the article, specifying that "Neither speech nor the press shall violate the honor or rights of other persons nor undermine public morals or social ethics. Should speech or the press violate the honor or rights of other persons, claims may be made for the damage resulting therefrom". This *caveat*, with its wide breadth and undefined limits, is a first breach in the system, empowering the South Korean authorities to impose restrictions to those rights.

The country's legal system as a whole is quite complex, and composed of numerous specific regulations and laws. The government began to regulate mass media in the 1980s. The *Basic Press Law*[75] authorized significant *censorship* activities; subsequently, however, this law was repealed following the emanation of the 1987 *Periodical Act*, regulating printed materials, and the 1987 *Broadcast Act*, regulating all broadcast media.

As mentioned above, South Korea has a rich and developed legal system. With regard to the country's *media*, it is first necessary to point out that there are two principal branches of South Korean media legislation: the first regulating all market and business aspects, and the second addressing media content. The two most important pieces of legislation governing the business aspects of media are undoubtedly the *Internet Multimedia Broadcasting Business Law* and the *Telecommunications Business Act*, which have sparked intense debate regarding both technical and legal matters. Debates centered on Article 47[76], which establishes significant criminal sanctions for the distribution of "false" information, but, above all, on Article 53,[77] which was, in fact, repealed in 2007. This article empowered the government to engage in censorship activities in the event of "harmful" content, establishing that such content was to be determined by presidential decree. In 2002, however, the Korean Constitutional Court intervened, ruling that the section in question was insufficiently specific and clear and granted the government excessive regulatory and decisional powers.[78] Subsequently, the government amended the section in question, adding the term "illegal" to the description of content that might be censored.

---

[75] Article 3 states: "Article 3 provides: 1. The press shall respect the dignity and value of human beings and the basic democratic order; 2. The press shall perform its public duties by contributing to the formation of democratic public opinions concerning matters of public interest by means of news reports, commentary, and other methods; 3. The press shall not infringe upon the personal honor or rights of an individual, or public morality or social ethics; 4. The press shall not encourage or praise violence and other illegal actions which disrupt public order".

[76] Article 47 of the Telecommunications Code states that it is illegal to "disseminate false news intended to damage the public interest." The penalty for any violation can mean up to 5 years in prison. The electoral law was amended in 2004 to prohibit the dissemination via the Internet of defamatory statements about politicians running for office in an election campaign. The Penal Code, notably the provisions against insult and defamation – even when the statements turn out to be true – is also used against Internet users (Article 307).

[77] Article 53 declares: "a person in use of telecommunications shall not make communications with contents that harm the public peace and order or social morals and good customs".

[78] See the decisions of the Korean Constitutional Court, Opinion 14–1 KCCR 616, 99Hun-Ma480, June 27, 2002, at http://www.ccourt.go.kr/home/english/decision_etc./decision2003.htm. Accessed 14 November 2011.

With a modification made in 2007 to the so-called *Information Act*, the provision in question, while still formally in force, in practice lost its legal effect.

There are, then, numerous laws, that while not specifically designed to regulate the media, have wide applicability and thus effectively authorize censorship by the state; of particular note are the *Juvenile Protection Act*, the *National Security Law* (NSL)[79] and the *Election Law*. On the basis of the above laws, the many Korean institutions operating in the communications sector[80] have wide intervention powers, including filtering and site and ISP address blocking activities.

Also noteworthy, in terms of South Korea's legislation, is the 2009 "three strikes" provision regarding copyright violation. Article 133[81] of the *Copyright Law* confers upon the Minister of Culture, Sport and Tourism the right to remove content, and to cancel Internet access for those subjects who repeatedly engage in activities involving copyright infringement.

Clearly the situation in South Korea does not approach the alarming levels found in North Korea. However, it is among the countries that are "under surveillance" by the organization *Reporters Without Borders*. Its convoluted and, in some cases, excessively generic, legal framework, in addition to its multiple control bodies, renders state limitations of the freedom of speech quite invasive. Diverse investigations have documented considerable censorship activities regarding content pertaining to North Korea. Internet crackdowns have been reported, particularly in 2010 when a number of sites covering a series of popular revolts were obscured. A recent reform to a piece of legislation known as the *Network Act* would require users to register under their full names when visiting portals with over 100,000 members. This has resulted in intense protests, in addition to the blocking of the Korean *youtube.com* site.

One final case should be cited, that of the persecution of one of South Korea's myriad active bloggers. The well-known blogger Park Dae Sung, who is known as *Minerva* on the web, was accused of circulating false information and of having criticized the government's economic policy. Fortunately, after a period of detention, a Seoul District Court absolved the blogger of "distribution of false information". The court has not yet released an explanatory memorandum for the case, but it is known that the prosecuting attorney had requested an 18-month prison term.

---

[79] See the Article 7 of the National Security Law, that prohibits promoting or encouraging anti-statist groups, including North Korea. In paragraph 5 of this Article, any publication in support of the enemy or the mere reprinting of a document on the subject is also prohibited. Article 8 also prohibits any contact or communication with anti-statist groups. Recently the police investigated a cybercafé from which pro-North Korean messages had allegedly been posted. The café's owner was charged with violating the National Security Law.

[80] See the Korean Communitations Commission, the Korean Broadcasting Commission, the Korean Communitations Standard commission.

[81] See the text of Article 133: "Collection, Abandonment, and Deletion of Illegal Reproductions," "the Minister of Culture, Sports, and Tourism would be authorized to shut down message boards that refuse to comply with more than three warnings to remove copyrighted content, while users who upload such content may also have their accounts canceled"

6.2.4 *Saudi Arabia: The Digital Liberties Landscape*

The Arabian Peninsula has been identified as one of the 15 geographic regions in which it is hypothesized that human society and culture originally organized, and was not only the birthplace of the Prophet Mohammed, but also the cradle of Islamic culture and civilization. The modern nation of Saudi Arabia was founded in 1932 by King Abd-al-Aziz Ibn Saud (known as the *Lion of Najd*) and is an absolute monarchy. The monarch is both of Head of State and the country's supreme religious leader, and is thus in a position of nearly absolute power. Only male members of the royal family may be considered for succession to the throne and succession is governed by the unwritten rule of "seniority"; the highest political roles are occupied by the most influential members of the same family.

The refusal by the regime to tolerate any form of opposition has encouraged, in recent years, the growth of extremist groups such as al-Qaeda. This organization, which owes a good deal of its popularity to the figure of Osama Bin Laden, has benefitted from the popular resentment against the role of the United States in the Middle East, and it is unfortunately no coincidence that the individuals who carried out the terrorist attacks of September 11, 2001 were nearly all Saudi citizens. Thus in recent years the regime has come under increasing pressure to introduce political reform. In 2005 the country's municipal elections were a first, limited exercise in democracy; however, currently political parties are still forbidden, any opposition activities must be organized from outside the country and journalism is tightly controlled.

Saudi Arabia possesses over 25% of the world's oil reserves, and produces approximately ten million barrels per day. The population is approximately 26 million, and of these just over 11 million connect to the Internet.[82] The *media* environment in Saudi Arabia is in all likelihood that which is most severely controlled in all the region. The television networks and stations are all operated by the state-owned *Broadcasting Service of the Kingdom of Saudi Arabia* (BSKSA),[83] which is chaired by the Minister of Culture and Information.

The regime's global filtering system is able to block thousands of sites including those addressing political, social or religious issues. Recently a number of Saudi studies revealed that there are nearly 10,000 *blog*s in the kingdom.[84] Unfortunately, in 2009 the *Committee to Protect Journalists* classified Saudi Arabia as the fifth-worst country in which to be a blogger, and it is among the top ten "Internet Enemies" according to the organization *Reporters Sans Frontières*.[85]

Saudi newspapers are established by decree. New regulations designed to strengthen censorship and to discourage the use of Internet for the publication of news or for blogging were announced on 1 January 2011 by the Minister of Culture and Information, Abdul Aziz Khoja. Pursuant to Article 7 of the law, online media and the

[82] See http://www.internetworldstats.com/middle.htm#sa. Accessed 21 November 2011.

[83] See http://www.info.gov.sa/English/eSectDetails.aspx?id=12. Accessed 21 November 2011.

[84] See http://news.bbc.co.uk/2/hi/middle_east/country_profiles/791936.stm. Accessed 21 November 2011.

[85] See http://en.rsf.org/internet-enemie-saudi-arabia,39745.html. Accessed 21 November 2011.

Internet platforms offering audio and video content must now first obtain an "Internet license" which must be renewed every 3 years. Applicants must be Saudi nationals, aged at least 20, have a high school diploma and must be able to produce "documents testifying good conduct". These measures are clearly discriminatory. The age and degree requirements deprive thousands of young people of their right to free expression, while foreign residents are excluded by the citizenship requirement.

Online sites must indicate the names of their hosts them, so that the government may, at any time, pressure the server to eliminate the site or its contents. All blogs, personal web sites, electronic archives and chat rooms must register users, the intention of the government obviously being that of eliminating web anonymity. According to Article 17, any violation of these provisions is subject to severe punishments (100,000 Saudi Ryals, or nearly 20,000 euros) and a partial or total block of the web site, which may be permanent. The Ministry reserves the right to increase any of these measures.

According to a law regulating the use of technology, that came into force in January 2008, operating a web site advocating terrorism is punishable by up to 10 years in prison, the distribution of material that is pornographic or that violates public law or the realm's religious values may be punished with a prison sentence of 5 years while financial fraud and violation of privacy are subject to sentences of up to 3 years. The same laws establish prison sentences for the owners of Internet cafés, and any individual, suspected of being an accomplice to or who has consented their computer to be used in order to distribute information or contents that "violate the values of the Realm". Penalties for these offenses are equal to half those for the cases outlined above.

In 2008, the Ministry of Culture and Information, Iyad Madani, imposed a national ban on all live broadcasts on Saudi television. This was occurred just 2 days after an episode in which a number of viewers called in to complain on the news channel *Al-Ikhbariya*a bout the government's failure keep a promise to raise salaries. They targeted a number of senior Saudi officials, including the king, Abdullah bin Abdulaziz al-Saud.[86] The episode also resulted in the dismissal of the direction of the channel, Mohammed Al-Tunsi.

The Saudi government makes no attempt to hide its filtering activities; to the contrary it clearly illustrates the "service" in a section of the site "Internet Services Unit" managed by the Permanent Security Committee headed by the Internal Ministry.[87] According to this site, the "King Abdulaziz City for Science & Technology (KACST)"[88] is directly responsible for filtering all pornographic activity, while other sites are blocked at the request of "government security bodies". The web site also offers information regarding how users can request that certain sites or content be blocked. The site also specifies that other software packages allow "discreet" monitoring and tracking of all web pages visited by a determined computer or imposition of time limits for internet use.

[86] See http://en.rsf.org/saudi-arabia-information-minister-bans-live-01-02-2008,25340.html. Accessed 21 November 2011.

[87] See http://www.isu.net.sa/saudi-internet/contenet-filtring/filtring.htm. Accessed 21 November 2011.

[88] See http://www.kacst.edu.sa/en/Pages/default.aspx. Accessed 21 November 2011.

The Saudi filtering system is extremely rigid. Access is prohibited to sites with pornographic or unfit content, featuring discussions of religious or human rights issues and to sites presenting the opposition's viewpoints. Far from hiding their actions, Saudi authorities openly document censorship activities and claim to have blocked thousands of sites, including the ANHRI (the *Arabic Network for Human Rights Information*), *gulfissues.net*, *saudiinstitute.org*, *arabianews.org*, Al Jazeera.org and *saudiaffairs.net*. Two other sites were blocked at the beginning of 2011 in reaction to the Tunisian and Egyptian revolutions; both, *dawlaty.info* and *saudireform.com*, advocated political changed in Saudi Arabia as well. The site *newarabia.org*, a political discussion forum, has been blocked and the its platform, *blogger.com*, which at first was totally inaccessible, is now strictly censored in terms of content. The Saudi religious police have expressed interest in online surveillance tactics and a number of members of the "Commission for the Promotion of Virtue and the Prevention of Vice" have asked the President of the Shura Council (an advisory board) to allow them to access blocked web sites in order to monitor the immoral practices by the visitors to those sites. According to data provided by Reporters Sans Frontierès the Saudi government has blocked more than 1,200 blocked Saudi sites.

The *Open Net Initiative* (ONI) conducted a number tests on three Internet Service Providers, *STC, National Engineering Services & Marketing (Nesma) and Arabian Internet and Communications Services (Awalnet)*. The three ISPs using the same centrally administered filtering system, Secure Computing's *SmartFilter*, block the same websites. The ONI additionally verified that, in line with the Saudi government's emphasis on protecting the "sanctity of Islam" and the legitimacy of the regime, several religious sites, relating to minority Shia groups and sites that espouse alternative views of Islam, were also blocked. Also blocked were numerous sites relating to alcohol and drug use, sexual habits and games. A consistent number of internet tools, including anonymizers and translators, were blocked as well.

In August 2010 Saudi authorities threatened to block the *BlackBerry* instant messaging service (*BlackBerry* phones are favored by dissidents due to the company's high security levels), and exerted enormous pressure on *Research in Motion* (RIM), *BlackBerry*'s producer, to provide access, albeit with some degree of legal guarantees and through a court order, to *BlackBerry* user message data. As a result of the pressure, RIM agreed to install a server in Saudi Arabia (up to that point all company servers had been located in Canada) in order to not risk losing such an economically important market. Thus Saudi authorities, in possession of *BlackBerry* encryption keys, would be able to gain access, by means of a court order issued within the country, to determined messages relating to serious crimes, after the fact. However, in light of the determination with which the regime implements its censorship policies, in all likelihood *BlackBerry* users may expect the possibility of real time surveillance of their smartphones.

Draconian restrictions have been imposed on cybercafé operators as well. Since April 2009 they are now required to install hidden cameras,[89] to provide a list of

[89] See http://opennet.net/blog/2009/04/restriction-internet-use-middle-east-rise-internet-caf%C3%A9s-saudi-must-install-hidden-came. Accessed 21 November 2011.

customers and websites consulted and to close a midnight. They may not allow the use of prepaid cards or admit minors.

Sheikh Mekhlef bin Dahham al-Shammari, a writer, social reformer and human rights activist noted for his outspoken defense of women's rights and his efforts to reconcile Shiites and Sunnis has been in prison since 15 June 2010.[90] His arrest was connected to criticism lodged against the country's religious and political leaders, published on the web sites saudiyoon.com and rasid.com.

Mohammed Abdallah Al-Abdulkarim, a law professor and activist known for his efforts to defend political and civic rights, was arrested on 5 December 2010 in Riyadh. Following King Abdullah bin Abdulaziz Al Saud's medically motivated trip to the United States, Mohammed Al-Abdulkarim posted, on 23 November 2010, on the website royaah.net, an article mentioning differences within the royal family – specifically disputes over King Abdullah's succession and their consequences for Saudi Arabia's political future. In this post, he mentioned not only the King's state of health, but also the power struggle between the sovereign's potential successors.

There is still no news of Syrian blogger Raafat Al-Ghanim, a resident of Saudi Arabia who was arrested in July 2009. He openly criticized the Syrian and Saudi social and political situations on both countries' online forums.

Last, but not least, in November 2010, *Facebook* was blocked for several hours for having violated Saudi Arabia's moral values.

In 2012, the dissident Manal al-Sharif was honored for "creative dissent" at the Oslo Freedom Forum. As Sutter remarks (Sutter 2012):

> […] she gained international attention last summer after she uploaded a YouTube video of herself driving in a country where women are banned from doing so. Now she is the face of Saudi Arabia's Women2Drive movement, which plans to hold demonstrations on June 17 calling for women in that Middle Eastern country to be able to do something that's downright banal everywhere else in the world: drive themselves around town in an automobile. While driving is technically not illegal for women in Saudi Arabia, a religious edict, or fatwa, issued in the early 1990s, banned the practice. A statement from the Ministry of Interior backed up the decree […] Al-Sharif's act of defiance did not go unnoticed. The next day, police detained her. She was held for nine days without being charged, she said, and then released after considerable international pressure, much of it coming from the Twitter hashtag #Women2Drive and corresponding pages on Facebook. The next month, on June 17, dozens of women in Saudi Arabia got behind the wheel and drove to protest the ban, according to news reports. (Sutter 2012).

6.2.5 Syria: Digital Liberties Issues

The Arabic Republic of Syria has been governed by the Ba'th party since 1963 and a member of the Assad family has held the role of Head of State since 1970. Currently Syria is going through one of the most dramatic moments in its recent history.

[90] See http://en.rsf.org/saudi-arabia-human-rights-defender-held-since-22-07-2010,38000.html. Accessed 21 November 2011.

In the first few months of 2011, during what has come to be known as the "Arabian Spring", a number of popular uprisings flared in various regions throughout the country, but after an initial period in which it appeared that the government might concede to requests for certain reforms, President Bashar al-Assad's government began a series of bloody military crackdowns and episodes of severe repression, which appear to be leading the country ever closer to civil war.

The military has regularly fired into crowds of peaceful protesters and has bombed entire residential neighborhoods. The regime hopes to re-establish order and to regain control of the country through the indiscriminate use of military force. Since the beginning of the outbreak to the time of this writing, in the autumn of 2011, over 3,000 people have been killed, including at least 187 children, according to information provided by the UN High Commissioner for Human Rights, Navi Pillay.[91] Additionally, there have been reports of thousands of arrests, disappearances, cases of torture and rape by government forces. The leaders in Damascus, well aware that among the approximately 24 million Syrians there are at least five million Internet users, have intensified their efforts to control and monitor the web, to identify dissidents on social networks and to impede the circulation of any online news and information backing the anti-government protesters (web pages in support of anti-government are frequently assailed with a barrage of pro-Assad messages). Despite many promises made to the Syrian people in the past, it is now quite clear that the government hopes to stay in power at whatever cost, and has no intention of yielding to requests calling for a gradual shift towards a more democratic system. At the beginning of October 2011, both China and Russia voted a draft resolution of the UN Security Council calling for an end to human rights violations and for the referral to the International Criminal Court for investigation of crimes against humanity committed by Syrian authorities.[92] Subsequently, Ahmad Bader Hassun, Syria's Grand Mufti (not so much a religious as a political position), threatened to launch suicide attacks against both the EU and the United States in the event of any Western military attack against the Damascus regime. The repercussions of these events throughout the Middle East are clearly worrisome, all the more so because Syria is, not least because of its central location in the region, a country of enormous strategic importance for the numerous and highly delicate geopolitical balancing acts that are so typical of the region's political landscape.

The Syrian Constitution establishes, in Section 4, entitled *"Freedom, Rights, Duties"*, the following relevant provisions[93]: Article 25 (Personal Freedom, Dignity, Equality): "Freedom is a sacred right. The state protects the personal freedom of the citizens and safeguards their dignity and security". Article 32 (Secrecy of Communication): "The privacy of postal and telegraphic contacts is guaranteed." Article 38 (Expression): "Every citizen has the right to freely and openly express his

[91] See http://www.un.org/apps/news/story.asp?NewsID=40046&Cr=Syria&Cr1=. Accessed 21 November 2011.

[92] See http://www.un.org/apps/news/story.asp?NewsID=39935&Cr=syria&Cr1=. Accessed 21 November 2011.

[93] See http://www.servat.unibe.ch/icl/sy00000_.html. Accessed 21 November 2011.

views in words, in writing, and through all other means of expression. He also has the right to participate in supervision and constructive criticism in a manner that safeguards the soundness of the domestic and nationalist structure and strengthens the socialist system. The state guarantees the freedom of the press, of printing, and publication in accordance with the law." Article 39 (Assembly): "Citizens have the right to meet and demonstrate peacefully within the principles of the Constitution. The law regulates the exercise of this right."

Formally, therefore, the freedoms of speech and of the press and the rights to the confidentiality of correspondence and of peaceful assembly are all guaranteed by the Constitution, but in actual fact the government in Damascus limits them severely, with repressive laws such as the 1962 Emergency Law, in addition to numerous others designed to censure diverse forms of communication. The Press Law, for example, establishes wide control over all materials printed in Syria, while Articles 286 and 287 of the Criminal Code punish the distribution of foreign news, and Decree no. 6 of 1965 prohibits the publication of any news designed to inspire revolutionary sentiments among the populace. As previously mentioned, Syrian authorities have extended censorship activities to the internet and since March 2008 the country's Internet cafés are subject to a series of measures so stringent that opening an Internet café becomes not only difficult, but even dangerous. Thus anybody wishing to do so must first obtain a license from the Ministry of Telecommunications and Technology,[94] and must then obtain security clearance from the Ministry of the Interior establishing compliance with all Internet café security directives, which include the annotation of identification documents not only of every café client, but even of their parents as well. All Internet café owners are obliged to conserve a register documenting all clients and to clearly post warnings that no religious or political sites may be consulted; failure to observe these regulations may result in heavy fines, the closure of the establishment and even prison. According to a number of reports from Internet café owners, Syrian authorities provide special software programs to monitor client web use.

The Ministries of the Interior and of Telecommunications have prohibited the sale of mobile telephones utilizing GPS and WAP when those services cannot be fully monitored by the service providers.[95]

In 2010, a bill clearly designed to further limit the circulation of information on the Internet was approved by the Council of Ministers and rushed through Parliament in record time. Two provisions of the new law are particularly alarming: the first establishes harsh prison sentences for journalists, while the second permits authorities to investigate journalists for having committed "crimes" and to decide whether or not they should be arrested. The new law is a reaction to the rapidly growing presence of new media in Syria in recent years, which are clearly seen as a threat by the authoritarian regime.

While Internet access has significantly increased over the last decade, the existing infrastructure has remained virtually identical. Thus connection slowdowns and outages (bottlenecks) are frequent. Connections are also quite slow, with most users

[94] See http://www.ste.gov.sy/. Accessed 21 November 2011.

[95] See http://opennet.net/research/profiles/syria. Accessed 21 November 2011.

still restricted to a speed of 56 kb. DSL lines and 3 G connections are still expensive (although the 3 G network controlled by the Syriatel mobile telephone company,[96] owned by Rami Makhlouf, a cousin of the president, is experiencing strong growth). It is not unreasonable to think that the persistence of this state of affairs is a deliberate strategy to keep the country's population away from the Internet.

According to *Reporters Sans Frontières*,[97] Syria ranked 173rd (out of a total of 178 countries) in the 2010 Press Freedom index, and is considered one of the top ten "Internet enemies".

In an effort to stem the impact of Internet use by the regime's opponents, Syria has adopted a number of strategies that differ from those of other countries involved in the "Arabian Spring" of 2011. Without changing its generally repressive approach, it first unblocked a number of popular social networking sites and subsequently, with the aid of groups of pro-government expert computer technicians (for example, the Syrian Electronic Army and the Syrian Electronic Soldiers[98]), initiated a series of activities to combat the opposition forces online with systematic counter-information techniques directed at both domestic and western media. Thus Syria is the first state to have created a true cyber army ready to launch attacks against anti-regime groups and western websites, defacing websites and flooding forums, blogs and online chat sites with spam and pro-regime messages. They identify themselves as "*a group of enthusiastic Syrian youths who could not stay passive towards the massive distortion of facts about the recent uprising in Syria, and this distortion is carried out by many Facebook pages that deliberately work to spread hatred and sectarian intolerance between the peoples of Syria to fuel the uprising*". The following data has been documented by the Information Warfare Monitor (IWM),[99] an independent research organization specializing in tracking cyberspace strategic activities, seeking to broaden the evidence base available to scholars, policy makers and researchers.

The Electronic Army has claimed responsibility for at least 50 Syrian websites, including that belonging to the popular singer Asalah Nasri, who had refused an invitation to perform at a concert in support of President Bashar al-Assad. Moreover, a number of *defacement* attacks have carried out against western websites as well, including the Italian sites http://bluereef.it,[100] http://www.windcam-news.it/usato.php[101] and http://aguide2italy.com.[102] In these particular cases such actions would appear rather inefficient, given that these sites are in reality simply on-line stores

[96] See http://syriatel.sy/. Accessed 21 November 2011.

[97] See http://fr.rsf.org/. Accessed 21 November 2011.

[98] See http://www.syrian-es.com/. Accessed 21 November 2011.

[99] See http://www.infowar-monitor.net/?s=syria. Accessed 21 November 2011.

[100] See http://www.infowar-monitor.net/wp-content/uploads/2011/05/SEArmy-Figure-6.png. Accessed 21 November 2011.

[101] See http://www.infowar-monitor.net/wp-content/uploads/2011/05/SEArmy-Figure-7.png. Accessed 21 November 2011.

[102] See http://www.infowar-monitor.net/wp-content/uploads/2011/05/SEArmy-Figure-8.png. Accessed 21 November 2011.

without any particular connection to any aspect of the conflict in Syria. It is therefore not clear whether the attacks were due to lack of comprehension of the Italian language, or rather because the Italian sites were particularly vulnerable to attack. At last report, the Electronic Army had organized spamming attacks against the Facebook pages of the European Parliament, the European Union, the Whitehouse, the US State Department, US President Barack Obama, French President Nicolas Sarkozy, Oprah Winfrey, Human Rights Watch, Al-Jazeera, Al-Arabia and others. The *OpenNet Initiative*, with the objective of investigating, exploring and analyzing Internet filtering and surveillance practices worldwide, conducted a number of tests[103] in 2009 and found pervasive political filtering. The ONI tests revealed that a number of Syrian blogs hosted on Google's popular blogging engine (blogspot.com) were blocked. Additionally, diverse websites for important Arabic newspapers and news portals were also unreachable, including Al-Quds al-Arabi (www.al-quds.co.uk) and Al-Sharq al-Awsat (www.asharqalawsat.com), the Kuwaiti paper Al Seyassah (www.alseyassah.com), and the American newsite Arab Times (www.arabtimes.com). Several Israeli websites were tested in order to verify whether Syria filters sites from the .il domain. In fact, none of the websites were accessible, suggesting that the Syrian government blocks the entire .il domain, without exception.

Recently, a number of "agents" (so they define themselves) from Telecomix[104] (hackers in the true sense, belonging to a group with no hierarchical structure), closely examined the Internet filtering technologies used by the Syrian regime and made some surprising discoveries.[105] They discovered that it is Blue Coat Systems,[106] a California-based firm and industry leader in web security products, that provides the Syrian government with the systems used by the regime to block websites and to interrupt secure connections with social networks in an effort to keep a tighter grip on its population.[107] In fact, information gathering activities conducted by Telecomix agents revealed at least 15 active Blue Coat systems. It is worthwhile to note that after Blue Coat, in an official company statement,[108] issued a staunch denial of ever having

[103] See http://opennet.net/research/profiles/syria. Accessed 21 November 2011.

[104] See http://telecomix.org/. Accessed 21 November 2011.

[105] See http://reflets.info. Accessed 21 November 2011.

[106] See http://www.bluecoat.com/. Accessed 21 November 2011.

[107] See http://reflets.info/bluecoats-role-in-syrian-censorship-and-nationwide-monitoring-system/. Accessed 21 November 2011.

[108] "Blue Coat does not sell to Syria and neither do we provide any kind of technical support, professional services or software maintenance. To our knowledge, we do not have any customers in Syria. U.S. companies are prohibited from selling to Syria. In addition, we do not allow any of our resellers, regardless of their location in the world, to sell to an embargoed country, such as Syria. We have seen logs posted that are allegedly from a Blue Coat appliance in use in Syria. From these logs, we see no firm evidence that would determine there is Blue Coat equipment in Syria; in fact, it appears that these logs came from an appliance in a country where there are no trade restrictions. In addiction, the log files appear to have come from a third party server that was storing log files uploaded from one of our appliances. The allegation that an organization penetrated one of our appliances through a security hole is flatly not true. There are no known vulnerabilities of our appliance that would allow such an action".

deployed their filtering appliances in Syria (in the past the firm had in fact stated that "*company policy prevented the sale of such devices to the Syrian government*", additionally citing the US embargo against Syria in force since 1986), 54 gigabytes of logs[109] from Blue Coat devices, accompanied by detailed graphic support,[110] were promptly published online. As it that were not sufficient, a community social engineering campaign examined the LinkedIn profiles of a number of computer technicians, revealing that many of their work histories include work experience in Syria, where they specialized in installing Blue Coat devices for hundreds of Syrian clients.

The evidence collected by Telecomix agents clearly demonstrates the existence of filters to several communication services, including MSN, Yahoo Messenger and Facebook chat, and further, and more ominously, revealed that Syrian authorities can easily obtain user passwords and monitor any and all communication that takes place.

Syrian authorities actively engage in the legal persecution of the country's cyber-dissidents.[111] For example, Habib Saleh was tried in December 2008 for having published articles calling for democracy in Syria on the site www.elaph.com, currently censored in Syria, and was sentenced to a 3-year prison sentence in March 2009. Saleh was convicted pursuant to Article 285 of the Criminal Code for "*weakening national sentiment*", an accusation, however, that is applicable only in times of war.

In the same fashion, the blogger Tariq Biasi also received a 3-year prison term for "*weakening national sentiment*", and for "publishing false information" on his blog.

An attorney and editor of the website *Souleiman* Ali Abdallah was detained for 12 days for "*persisting in publishing legal and political articles criticizing the role of the government*" in his website alnazaha.org.

The accusation of false information leading to the weakening of national sentiment is often used by authorities against journalists and netizens, as in the case of the blogger Karim Arbaji, sentenced to a 3-year prison term in 2007. Two additional netizens, Kamal Hussein e Cheikhou Ben Tal Al-Mallouhi, are currently still behind bars. The laws currently in force allow authorities to try before a military court even civilians who are under the mere suspicion, without any proof whatsoever, of having committed "crimes constituting a global danger" (so vague a concept as to cover a multitude of activity). Existing press laws prohibit websites from publishing any political content and bloggers may risk heavy sanctions or prison terms. Finally, according to information released in September 2011 by Reporters Sans Frontières, Najati Tayara, a human rights activist arrested at Homs on 12 May 2011 was released only on 29 August, while Anas Al-Morawi, a blogger arrested on 1 July 2011 in Damascus, was released on 28 August.

Still in prison are Omar Al-Assad, Sami Al-Halabi, Hanadi Zahlout, the bloggers Jehad Jamal Othman and Rudy Asim Hamsho, and various netizens, including Abd

[109] See http://tcxsyria.ceops.eu/95191b161149135ba7bf6936e01bc3bb. Accessed 21 November 2011.

[110] See http://hellais.github.com/syria-censorship/. Accessed 21 November 2011.

[111] See http://cyberdissidents.org/bin/dissidents.cgi?id=64&c=SY. Accessed 21 November 2011.

Qabani and Ammar Sa'ib, Manaf Al Zeitoun, Mohamed Jamal Tahan, Abd Al-Majid Tamer and Mahmoud Mohamed Al-Asem.

In 2011 the EFF raised concerns about the efficiency of export controls referring Syria as one of the most problematic countries. Alongside the cited Blue Coat company, recently the Italian company Area SpA had contracted with Syrian intelligence agents to develop a surveillance system with the power to intercept, scan and catalog virtually every e-mail that flows through the country, to the alleged price tag of 13 million euros. The system, writes EFF, included components made by Sunnyvale-based company NetApp Inc., as well as by German company Utimaco Safeware AG and Hewlett-Packard equipment. Last but not least, EFF remarked that also Syrian Addounia TV, under sanctions by both Canada and the EU for inciting violence against Syrian citizens, uses Canada-based servers to host its website and Al-Manar, the official television station of Hezbollah banned by Canada and EU, and on the United States' Specially Designated Nationals List, hosts its website on US and Canadian servers as well. Syria, outlines EFF, is unique in that the export of technology to the country falls under several different sanctions regimes in the United States alone. Canada has enacted similar controls, but also allows for exceptions through special licenses granted by the Minister of Foreign Affairs. EU sanctions are more specific, targeting mainly individuals and companies. They continue to be expanded, most recently to targeting two members of the Syrian Electronic Army. But the same export controls meant to prevent the Syrian regime from accessing the aforementioned technology also frequently prevents Syrian citizens from getting their hands on technology that they need. EFF has described how export regulations prevent Syrians from downloading popular tools like Google Chrome and Google Earth, and from using Skype to call their families abroad (Syrians can use Skype, but they can't add credit to their accounts and are therefore limited to Skype-to-Skype calling).[112]

6.2.6 Iran: Internet and Digital Liberties Issues

6.2.6.1 Internet Use in Iran

Internet use in Iran is expanding rapidly. The number of Internet users in Iran has gone from fewer than one million in 2000 to approximately 23 million in 2008; this level of growth is the highest of all the countries in the Middle East and the level of Internet penetration, 35% in 2009, is considerably higher than the regional average (26%).[113] With its approximately 60,000 active blogs, the Iranian blogosphere is

[112] See https://www.eff.org/deeplinks/2011/11/sanctions-fail-stop-syrian-regime-still-harm-citizens. Accessed 23 November 2011.

[113] See the 2009 ONI Report *Internet Filtering in Iran*, http://opennet.net/research/profiles/iran

among the world's most active, an incredible number considering the rigid control that the country's authorities keep over the Internet.

Following a significant increase of online political organizing prior to and during the 2009 presidential elections, the Iranian government initiated a true war against Internet liberties, adopting numerous and highly sophisticated measures that go far beyond simple content filtering.

Efforts to control of the freedom of expression involve every type of communication, from traditional media, to the media and satellite transmissions and implements diverse typologies of censorship at various levels.

The architecture of the Internet in Iran facilitates this control; private ISPs are forced to use wideband services furnished by the government or to direct their traffic through filtering systems developed by Iranian companies. The *Committee in Charge of Determining Unauthorized Websites* (CCDUW) is legally responsible for the identification of web sites that contain prohibited content and refers this information to the Telecommunication Company of Iran (TCI – the state provider of Internet and mobile telephone services) and to the various ISPs so that they may proceed to block the offending sites.

The ISPs, which can operate only if authorized to do so by the TCI and the Ministry of Culture and Islamic Guidance, are obliged to follow all state directives and are responsible for all content they transmit. In 2010 Iranian authorities issued a "List of Internet Offences", drawn up by a committee of experts, which served to increase the already pervasive and rigid Internet filtering. The list was an inventory of forbidden behaviors, identifying for punishment all content that is contrary "to the morals of society", "to religious value", "to security and social peace" or that is "hostile towards government officials and institutions", or that "facilitate the commission of a crime", including technologies and applications that function to evade censorship systems.

Moreover, from 2006 onward, the government has ordered all ISPs to limit their downloading speeds to 128 kbit/s for all connections, both domestic and those located in Internet cafés. This measure, which limits the possibility of users to download multimedia content, is clearly an attempt to render the Internet less attractive and, consequently, to direct users toward other, more easily controlled, sources of information. Currently Iran is the only country in the world to have set a maximum ceiling for connection speeds. If to this is added the fact that connection costs are kept deliberately high, it is quite clear that in Iran there are still considerable obstacles to accessing the Internet.

6.2.6.2 Surveillance and Censorship Activities

Censorship in Iran is implemented through the use of URL keyword blocking. In recent years the state has spent copious resources in order to develop filtering software produced domestically, in order to reduce its dependence on foreign software companies, who recently have begun to refuse to provide their filtering products to states

using them for arbitrary and indiscriminate censorship.[114] Iran filters a wide range of web sites considered offensive for the moral standard of the Islamic state; site supporting the political opposition, women's and minority rights and human rights in general are commonly targeted. A primary objective of censorship is constituted by *political opinion* that is contrary to the government. The limitations to the freedom of political expression was made quite evident by the Guidelines issued for the 2009 elections, which expressly prohibited 20 categories of speech, including any discourse "disrupting national unity" or "creating negative feeling forwards the Islamic government".

According to *Open Net Initiative* reports, independent and western media sites are constantly inaccessible,[115] as are web sites for numerous international human rights organizations, such as *Amnesty International*, and sites fostering liberties in general, such as *OpenNet* itself. Blocked as well are many popular web sites for social networking, even Iranian social networks,[116] and sites promoting rights for ethnic and religious minorities, especially those supporting Kurdish minorities. Content featuring any materials involving pornography, homosexuality, drug use, arms and alcohol is subject to harsh censorship and filtering. This last type of censorship is so severe that it frequently results in unintentional overblocking. Websites offering tools and technologies for evading censorship are naturally filtered and inaccessible from within Iran. As always, it is interesting to examine some of the actual keywords blocked by the state. In Iran, not only are no results retrieved for web searches including the word "sex", but block messages are also received for searches for the word "women" and even for the Farsi word for "photograph".

In addition to censorship, the government has spent considerable effort and resources to extend state propaganda to the digital sphere as well. Thus in Iran there are nearly 400 news sites directly or indirectly supported by the state. These sites feature news, commentary, and often outright propaganda in support of the government. Finally, self-censorship is unfortunately quite common in Iran. News of the arrest of bloggers, journalists and activists during protests and the perception of pervasive surveillance has created a climate of fear; this fear is the primary cause for the sacrifice of the freedom of expression.

6.2.6.3 Repressive Actions

In January 2011, authorities in Teheran announced the creation of a genuine cyber-police force to further tighten the grip of Internet control throughout the country. The Iranian "Cyber Army" has been fundamental in the arrest of hundreds of netizens.

---

[114] See the report ONI "*West censoring East. The use of western technologies by Middle East Censors"* at the address http://opennet.net/west-censoring-east-the-use-western-technologies-middle-east-censors-2010-2011

[115] See Al Arabiya, New York Times, Global Voices and BBC web sites.

[116] See Facebook, Twitter, Myspace, Flickr and local language social network like Balatarin, Orkut and Bebo.

The repression of Iranian netizens holds several unfortunate records: in addition to record numbers of sanctions handed down to the country's web users, the world's youngest blogger to be arrested and detained lives in Iran, and Iran is the only country to have executed bloggers for the content of their writings. Second only to China for the number of death penalties carried out, in Iran 2010 two website administrators, Saeed Malekpour e Vahid Asghari, were put to death for "agitating against the regime" e "insulting the sanctity of Islam".

In 2011 Iranian authorities arrested Navid Mohebbi, aged 18, the youngest blogger in the world to be incarcerated. The youngster, a defender of women's rights, was accused of "activities contrary to national security" and of "insulting the Islamic Republic's founder and current leader", and was also charged with being a member of the movement "One Million Signature movement to petition for changes in law that discriminate against women". His 3-year sentence caused international outcry, and the many petitions for his liberation, originating from every corner of the world, later led to his release on parole.

In 2012, a Commission was created, within the cyber-police, to block illegal VPNs in Iran. As Burleigh notes (Burleigh 2012):

> Iran's cyber police force is poised to launch a new crackdown on software that lets many Iranians circumvent the regime's Internet censorship […] The operation will target VPNs, or Virtual Private Networks, which use a secure protocol to encrypt users' data, foiling online blocks put in place by Iran's authorities […] About 20 to 30 percent of (Iranian internet) users use VPN, or more than seven million people out of the country's 36 million web users […] Legal VPNs would only be used by 'the likes of airlines, ministries, (state) organisations and banks' and even they would be monitored by the commission. Iran has long tried to stop its population accessing millions of foreign websites authorities see as undermining the Islamic regime, including Facebook, Twitter, the online pages of the BBC and CNN, many torrent sites, blogs, and pornographic hubs. 'Some websites are obscene and others are officially hostile towards the Islamic republic's system. (Thus), in the interest of the people and in order to prevent the collapse of families… there is blocking of the Internet', Hadianfar said. The Islamic republic's suppressing of the Internet has intensified since President Mahmoud Ahmadinejad was returned to office in a disputed 2009 election that sparked a wave of anti-government protests, mostly organised online. Many Iranian Internet users are used to getting around the censorship through the use of either VPNs or IP proxy software. But they are being increasingly hemmed in by more sophisticated measures being deployed by officials, who are planning a closed 'Islamic Internet' that some believe could be designed to supplant the world wide web within Iran. (Burleigh 2012).

6.2.6.4 Legal and Regulatory Frameworks

The censorship, the control, the surveillance and the repression described above are supported by a legislative structure that allows authorities to legally quash any unwanted behavior. The Iranian Constitution[117] provides for limited freedoms of

[117] Constitution of the Islamic Republic of Iran, (1979). See http://www.iranchamber.com/government/laws/constitution.php

opinion and expression, which, however, are not guaranteed in practice, due at least in part to legislation clearly designed to limit these rights.

The Constitution itself limits the freedom of the media, which may create a constructive forum for the encounter of different ideas, but must refrain from the diffusion of "destructive and anti-Islamic practices".[118]

The Press Law of 1986[119] the principal legislative instrument regulating the media in Iran. According to this law, the media are obliged to promote Islamic culture, contrast imperialist culture,[120] and must abide by precise limits[121] and respect numerous restrictions[122] in terms of content. The application of this law to blogs has been

[118] From the Preamble: "The mass-communication media, radio and television, must serve the diffusion of Islamic culture in pursuit of the evolutionary course of the Islamic Revolution. To this end, the media should be used as a forum for healthy encounter of different ideas, but they must strictly refrain from diffusion and propagation of destructive and anti-Islamic practices".

[119] See http://www.parstimes.com/law/press_law.html

[120] See Chapter 2: Mission of the Press. Article 2: The following constitute the objectives of the press in the Islamic Republic of Iran: (…) d. To campaign against manifestations of imperialistic culture (such as extravagance, dissipation, debauchery, love of luxury, spread of morally corrupt practices, etc.) and to propagate and promote genuine Islamic culture and sound ethical principles.

[121] See Chapter 4: Limits of the Press. Article 6: The print media are permitted to publish news items except in cases when they violate Islamic principles and codes and public rights as outlined in this chapter: 1. Publishing atheistic articles or issues which are prejudicial to Islamic codes, or, promoting subjects which might damage the foundation of the Islamic Republic; 2. Propagating obscene and religiously forbidden acts and publishing indecent pictures and issues which violate public decency; 3. Propagating luxury and extravagance; 4. Creating discord between and among social walks of life specially by raising ethnic and racial issues; 5. Encouraging and instigating individuals and groups to act against the security, dignity and interests of the Islamic Republic of Iran within or outside the country; 6. Disclosing and publishing classified documents, orders and issues, or, disclosing the secrets of the Armed Forces of the Islamic Republic, military maps and fortifications, publishing closed-door deliberations of the Islamic Consultative Assembly or private proceedings of courts of justice and investigations conducted by judicial authorities without legal permit; 7. Insulting Islam and its sanctities, or, offending the Leader of the Revolution and recognized religious authorities (senior Islamic jurisprudents); 8. Publishing libel against officials, institutions, organizations and individuals in the country or insulting legal or real persons who are lawfully respected, even by means of pictures or caricatures; and 9. Committing plagiarism or quoting articles from the deviant press, parties and groups which oppose Islam (inside and outside the country) in such a manner as to propagate such ideas (the limits of such offenses shall be defined by the executive by-law). Note: Plagiarism means intentional ascription of all or a considerable part of the works and words of others to one's own, even in the form of translation.

[122] See Article 7: The following activities are banned: a. Printing and publishing a publication without a license and a publication whose license has been cancelled, or, one which has been temporarily or permanently closed down by a court order. b. Publishing a publication the greatest part of whose items are incongruous to subjects which the applicant has undertaken to publish. c. Publishing a publication that may be mistaken in name, symbol or format for the existing publications or those which have been temporarily or permanently closed down. d. Publishing a publication without mentioning the name of its license holder and the legally responsible director or the address of the publication and its printing house. e. Publishing and printing houses, distribution and sales departments of publications are not permitted to publish and distribute publications which the Press Supervisory Board deems to be in violation of the principle stipulated in this by-law.

contested, but an amendment ratified in 2000 appears to have brought electronic publications under the aegis of the law. Another amendment adopted in 2009 removed all doubts, establishing that "the rules stated in this Press Law apply to domestic news sites and domestic websites and set out their rights, responsibilities, legal protection, crimes, punishments, judicial authority and procedure for hearings." Consequently, not only is online content subject to the same content limitations established for the press, but blogs and websites in general are now also required to obtain the same license prior to publication. Those who publish content without first obtaining state authorization are subject to the provisions of the Criminal Code,[123] and allows for imprisonment for those who disseminate false information and who create anxiety in the public's mind (Article 18) or who insult the government (Article 500)[124] or who distribute any form of propaganda against the state (Article 514).[125]

In 2009 Iran's Computer Crime Law went into effect, establishing imprisonment for computer crimes, defined as, among others, hacking, piracy, phishing, online defamation, and for the publication of any material that is deemed to be immoral or contrary to the public sentiment.

Since this law went into effect, the number of Persian bloggers to have been arrested, placed in isolation, tortured and sentenced after unfair trials and without the right to defense has increased.

This law also obliges ISPs to keep a record of all traffic for 6 months, and renders them liable for all content transmitted by users.

The legislative framework, destined to be further "enhanced" with additional, increasingly severe laws and regulations, plays a crucial role in rendering Iran one of the ten "Internet Enemy" nations, as reported by the organization Reporters Without Borders.

6.2.6.5 The Role of Internet in Social Mobilization for Democracy and Human Rights

Despite the country's legal framework, which is without a doubt terribly limited and even dangerous for Iranian citizens, the Internet remains the most important channel for expressing dissent against the actions of the government, and above all for uniting the country's activists and organizing pro-democracy social movements. This was precisely what occurred, as already mentioned above, during the 2009 elections, during which supporters for the opposition utilized the web to organize demonstrations against electoral fraud and against the repressive political climate, and calling international attention to the country's difficult political situation.

---

[123] See Islamic Penal Code of Iran (1996): http://mehr.org/Islamic_Penal_Code_of_Iran.pdf

[124] See Article 500: "Anyone who undertakes any form of propaganda against the State will be sentenced to between three months and one year in prison".

[125] See Article 514: "Anyone who somehow insults the founder of the Islamic Republic of Iran, Khomeini, or the Supreme Leader of the country should be sentenced to imprisonment from six months to two years".

But the web has demonstrated its positive potential in Iran on other occasions as well, and two in particular deserve mention. The first is known as the *"The One Million Signatures Campaign"* and was the first opportunity for Iranian women to assert their rights. Women in Iran are very much discriminated against by Islamic law, and for them the web represents for them a way to have their voice heard anonymously, and safely. Thus the One Million Signatures campaign, initiated in 2006, quickly grew as both men and women flocked to sign the petition requesting the end of inequality based on sex. Blogs, especially, have permitted Iranians to inform the world, with photos, videos, and news stories, of the campaign's progress and to provide updates on human rights violations against women in Iran, thus both promoting dialog and informing international human rights groups of events as they unfolded. Another campaign, known as the "Stop Stoning Forever Campaign", also created and conducted through blogs, had the objective of encouraging the government to end the practice of stoning. Article 99 of Iran's Sharia law in fact establishes that individuals committing adultery are to be stoned, and despite the fact that in 2002 the Ayatollah Shahroudi, the Head of the Iranian Judiciary, proclaimed a moratorium on stoning in Iran, this form of execution, contrary to universally recognized human rights, is still practiced in Iran. The digital campaign allowed the world to bear witness to the fact that this inhuman practice is still practiced in Iran, transmitting online videos and photos of executions. While it is true that neither of the campaigns have yet reached the practical results they strive for, since as yet there have been no changes to Iranian legislation, it is also true that they have both done a great deal in terms of alerting the international media to the plight of women and to the grave human rights violations in Iran, and above all have given hope to those who live these experiences directly, allowing them to believe in a means that will finally permit them to voice their dissent, and their pleas for help, outside the borders of their country.

Duncombe's study regarding social media, representation and crisis in Iran (Duncombe 2010) analyzed Western media coverage of the events surrounding the 2009 Green Movement protests in Iran. The author highlights four representational schemas (Duncombe 2010: 10) that were identified in the media coverage of these events:

1. that ICT platforms facilitate and accelerate democracy, and exposure to sites such as Twitter and Facebook is the real reason that apparently pro-democracy protests occur (not because desire for change was an indigenous movement) (Duncombe 2010: 10);
2. that public figures who use ICT platforms are necessarily pro-democratic (Duncombe 2010: 10);
3. that ICT are sources of *unadulterated truth*, despite the problematic nature of verifying sources (Duncombe 2010: 10);
4. the fourth representational schema works to coalesce non-Western protest movements (especially those that use ICT for information or communication) into a *homogenous wave of democracy*, wherein authoritarian regimes are toppled in favour of Western governmental structures (Duncombe 2010: 10).

Twitter's role in Iran's election crisis of 2009 continues to generate significant debate. Burns and Eltham noticed, in a recent essay (Burns and Eltham 2009), that *Twitter* users suddenly had mobilized, from all four corners of the world, to comment on Iran's electoral uncertainty and political future, and, after Iran's election result was announced on 12 June 2009, United States and Iranian activists turned to social media platforms, such as *Facebook* and *Twitter,* to protest (Burns and Eltham 2009: 303). As the scholars wrote, three points made clear the limitations of soft power and social media technologies for effecting social change:

1. *violence of the repression*. Those who championed the role of *Twitter* to spur the anti-regime social movement, the scholars remark, failed to understand or, worse, ignored the possibility that Iran's 'violence specialists' in its security apparatus would use *Twitter* to identify and hunt down pro-democracy protestors (Burns and Eltham 2009: 306);
2. *absence of counter-deception measures*. Iranian *Twitter* users did not take counter-deception measures to deal with the *Basij* (a para-military force), who then used *Twitter* to identify, locate and, in some cases, kill Iranian protestors (Burns and Eltham 2009: 306);
3. *unitended uses of the technology in a complex society*. The societal diffusion of a new technology platform, the authors note, inevitably means that different actors will exploit it for unintended uses, tactical advantages, and *systematic learning* (Burns and Eltham 2009: 306).

Sohrabi-Haghighat and Mansouri remarked that Iran's 2009 presidential election was so controversial for three fundamental reasons:

1. it came prominently into global media focus;
2. raised the suspect of large-scale frauds in the election that led to widespread protests, with the consequence of a repressive reaction from the regime and,
3. in the absence of independent media, news of the political upheaval was brought to the world by the protesters' extensive use of mobile phones and the Internet (Sohrabi-Haghighat and Mansouri 2010).

The scholars notes that, in the absence of independent media, and in the face of restrictive policies of the regime, which were evoked to inhibit any collective action, new technologies were used as effective communication tools allowing the protesters to solve organisational problems (Sohrabi-Haghighat and Mansouri 2010: 34).

Utilising the discursive opportunity afforded by the Internet, the *Green Movement* managed to enhance its political opportunities through extending its global reach, catching global media attention and raising human rights concerns (Sohrabi-Haghighat and Mansouri 2010: 34).

The regime's measures for controlling the circulation of information were abortive due to the resilient nature of the Internet, and new technologies allowed the opposition to maintain the protests and gave activists the opportunity to devise strategies and gain support on the web (Sohrabi-Haghighat and Mansouri 2010: 34).

6.2.7 *China: The Internet and Types and Levels of Chinese Internet Censorship*

6.2.7.1 General Overview

Despite the fact that the highest number of Internet users in the world are located within China's borders (with the country's Internet penetration rates nearing 35%),[126] this is also the country with the world's most sophisticated and efficient censorship systems, which place it firmly on the list of the top ten Internet Enemies published by the organization Reporters Without Borders.[127]

The data speaks for itself: the Chinese Communist Party, over the last decade has invested increasingly higher resources in technology, and for two quite different, even opposing, objectives. On the one hand, it seeks to perfect and modernize its national communications infrastructure, thereby not only making technology increasingly available to its citizens but also lowering costs; at the same time, however, the same government invests vast amounts in content filtering and control and in the development and maintenance of a structured, legalized and decentralized network for surveillance and control.

In recent years, China's economy, thanks in part to its investments in technology, has expanded significantly, and, at the same time, under the aegis of the Golden Shield Project promoted by the country's Ministry of Public Security,[128] it has implemented the largest and most sophisticated surveillance system in the world, known as the "Great Firewall" of China.

The Golden Shield Project was created to promote the adoption of advanced information technologies and to reinforce the ability of country's police to control, prevent and reduce crime. The project is constituted by instruments and technologies that allow it to watch, listen to and record virtually all communication by China's citizens. The portion of the project involving interception, filtering and censorship of the Internet is known (outside of China) as the Great Firewall of China, and while somewhat tongue in cheek, quite correctly indicated the virtual wall raised by the Chinese government against any aspect of the outside world that it does not consider appropriate.

The "Great Firewall" of China is in turn made up of numerous instruments, operating on diverse levels and from different angles, both preventively and in reaction to unapproved content, in both the physical and the virtual realities, both legislatively and using physical force.

---

[126] See "Freedom on The Net 2011" of Freedom House, Country Reports (China), http://www.freedomhouse.org/images/File/FotN/China2011.pdf

[127] See Reporters Without Borders, "Internet Enemies", March 2011, http://12mars.rsf.org/i/Internet_Enemies.pdfhttp://12mars.rsf.org/i/Internet_Enemies.pdf

[128] Ministry of Public Security, "National Development and Reform Commission issues national approval for the 'Golden Shield' construction project at management conference," November 17, 2006, http://www.mps.gov.cn/cenweb/brjlCenweb/jsp/common/article.jsp?infoid=ABC00000000000035645.

The first point of control occurs at the infrastructural level. Internet access service, in the past monopolized by China Telecom, was liberalized and decentralized, so that clients may now chose between diverse private ISPs; in reality, Chinese Internet users connect to the "global" network passing through six gateways that are closely monitored by state agents; private ISPs may operate only if they possess an operating license from China's Ministry of Industry and Information Technology (MIIT); in order to keep this license, they must cooperate with the government in implementing all national policy, signaling any suspect activities to authorities in a timely fashion.

Due to these structural realities, the Chinese World Wide Web is often referred to as a closed, monitored web.

In terms of content, just in 2010 Chinese authorities shut down approximately 60,000 websites containing "harmful material" (pornographic) and nearly 350 million articles, photos, and video clips were removed.[129]

A first form of content filtering in China is constituted by blocks, at the level of the routers that connect the Chinese network to the world wide web, of the IP address (or addresses) of specific webservers. In recent years, servers hosting numerous sites for international media, social networking, blogging, vlogging and web hosting services have been filtered by the Chinese government; at times these block are based on clear political choices,[130] other times, the blocks may be only temporary, following or during certain political or social events unfolding within the country.

Blocks of determined IP addresses imply that all the sites hosted on the same server targeted by Chinese authorities may be frequently inaccessible as well.

The redirection of IP addresses, or DSN tampering, functions in much the same way, this tool, commonly called Red Head due to the red characters that may appear on the screen advising of the removal and redirection, not only blocks access to sites deemed inappropriate, but goes even further, substituting the web page sought with another, conforming to state principles. Thus the state imposes its own moral values, disregarding the rights of its citizens to free and impartial information and to the access to culture. It must additionally be added, as will be described in further detail below, that this manipulation of IP address is often not made clear at all, thus frequently users who have been redirected to a government approved site may not even know that their Internet use has been censored.

While DSN tampering and IP blocking are frequently used in other countries as well, China is the only country to currently use another complex filtering system, based on lists of forbidden keywords. This method of censorship consists of intercepting and blocking URLs and TCP packets containing certain keywords, while they are transiting through the system's routers. Once a forbidden keyword has been detected, all packet transmission between the sender and the receiver is immediately blocked for a certain period of time. This system examines HTTP, FTP and POP

[129] See http://www.reuters.com/article/idUSTOE6B

[130] See the web sites of Amnesty International, Reporters Without Borders, Human Right Watch, Wikipedia and Falun Gong web sites.

traffic, and, naturally, some the most involved sites are search engines, Google[131] foremost among them, given that their services are based precisely on keywords.

It will come as no surprise that, despite repeated government assurances that Internet censorship is implemented for national security purposes, among the "forbidden" words are *democracy*, *freedom* (and all compounds and derivatives, such as *Free-China* and *Free-Net*), *corruption, demonstration, strike, Falun Gong*, all words relating to the hated "Three Ts" (Tibet, Tienanman[132]

[131] As Masnik notes (Masnick 2012) "It's no secret that Google has a troubled relationship with China: at one point leaving the market entirely, and later going back but with significant limitations, though where Google tried to be as transparent as possible about when information was being censored on behalf of the Chinese government". Masnik reports an interesting (and discussed) statement of Google, published on the blog of the company, with sort of "strategies" to avoid censorships activities: "Last week, Google took another step, which was explained, somewhat cryptically, in a blog post about *better search* in mainland China. The company never comes out and says it, but it's basically hinting strongly at the fact that the Chinese government is censoring certain searches… and doing so in a way that basically blocks access to Google for a certain amount of time, if they catch you doing a 'questionable' search". (Masnick 2012). The way Google explains this strategy is interesting: "Over the past couple years, we've had a lot of feedback that Google Search from mainland China can be inconsistent and unreliable. It depends on the search query and browser, but users are regularly getting error messages like "This webpage is not available" or "The connection was reset." And when that happens, people typically cannot use Google again for a minute or more… We've taken a long, hard look at our systems and have not found any problems. However, after digging into user reports, we've noticed that these interruptions are closely correlated with searches for a particular subset of queries". Masnick notes that "Of course, they never say what that 'subset of queries' might be, but you can take a guess. The 'solution' is that, similar (though slightly different) to Google's 'autocomplete', Google, when accessed by Chinese mainlanders, will make suggestions on alternative searches that won't cause the user to be blocked from accessing Google" (Masnick 2012).

[132] Chin (Chin 2012) remarks that the censorship (and control) of the word Tiananmen caused several problems in China: "China's Internet monitors have unleashed a broad clampdown on online discussion of the 23rd anniversary of the Tiananmen Square crackdown, restricting even discussion of the nation's main stock market when the Shanghai Composite Index fell by 64.89 points—a number that made for an eerie allusion to the sensitive date: June 4, 1989. […] Censors minding China's popular Twitter-like microblogging service Sina Weibo this weekend began blocking a number of terms that could refer to the 1989 Tiananmen Square crackdown, an incident often referred to as June 4 or 64 in the Chinese-speaking world. […] Terms blocked by Sina Weibo included the Chinese characters for 'Tiananmen', 'square', and 'candle', and even seemingly innocuous words like 'today'. It also included numbers that could allude to the event, including 23 as well as combinations of 4, 6, 8, and 9. The clampdown spread to the business and financial world—where censorship is less often a concern—when the benchmark Shanghai Composite Index first opened at 2346.98, containing all the tricky numbers, and then ended it down 64.89 points. Sina Weibo blocked use of the terms 'index' and 'Shanghai Index'. […] Chinese stock investors monitor their share prices in Huaibei, east China's Anhui province, on Monday. The Shanghai Composite closed down 64.89 on Monday, evoking the date of the Tiananmen Square crackdown on June 4, 1989, and prompting China's Web monitors to block discussion of the stock market close online. A spokesman for Sina Weibo operator Sina Corp. didn't immediately respond to a request to comment. Because Chinese officials often pressure companies themselves to strictly regulate content, it is assumed the censors blocking the searches are Sina's own, but it was unclear whether the tighter reins of recent days were ordered up by Beijing. The Shanghai Composite Index includes hundreds of Chinese companies and would be nearly impossible to manipulate to reach a preset figure based on stock purchases or sales. A media representative at the Shanghai Stock Exchange said trading opened normally on Monday. He declined to comment further. Reuters quoted the exchange's chief technology officer as saying the matter was being looked into". (Chin 2012).

and Taiwan[133]) and even the expression *children of party leaders*; moreover, leading up to and following the awarding in 2010 of the Nobel Peace Prize to the Chinese dissident and author Liu Xiaobo, given his inability to leave China to accept his prize, the expressions *empty chair*, *empty stool* and *empty table* were all similarly blocked.

In addition to "automatic" censorship systems, however, the Chinese Communist Party has also created a complex system of human censors to manipulate content. In fact, 1,000 of government commentators monitor China's network, posting pro-government news pieces, opinions and comments that shed positive light on party policies in an attempt shape and sway public opinion. This veritable army is known the "The 50 cent Party". They are paid to write on blogs and portals, but also on popular media websites. There are so many (international estimates have put their number at least 30,000) that some say the government has even found a way to reduce unemployment figures.

In addition to posting pro-government materials, the work of this digital army also includes out and out censorship, consisting of trolling the web to find and remove any unacceptable content. Following the strict guidelines established by their supervisors, working with meticulous attention to detail, not least due to fear of repercussion should they miss even one example of unacceptable content, they prefer to remove the entire contents of packet containing questionable material rather than allow ambiguous content to circulate freely.

In this climate of pervasive surveillance, self-censorship constitutes the final level, and is widespread among both normal citizens, who actively avoid posting content, and both domestic and foreign companies operating in the telecommunications sector, which rather than risk losing the licenses allowing them to operate in the Chinese market, prefer to implement party directives.

---

[133] As Weiping Li reports (Weiping Li 2012), in Taiwan in 2012 "On June 1st, Facebook suspended the accounts of several Hong Kong activists, causing speculation that the suspension was related to the 23rd anniversary of Tiananmen Protest in the absence of any other clear information or explanation from the company. Coincidentally, several Taiwanese activists and politicians also had their accounts suspended on the same day, which triggered Taiwanese users' concern over the limitation on free speech. Ho Tsung-hsun, the activist who has long devoted to social movements in Taiwan, posted an article describing the incident on the citizen journalism platform Peopo. According to Ho, after he saw the notice page of deactivation on Facebook, he clicked the FAQ link and tried to look for the reason of the suspension. Facebook listed four general reasons for account deactivation which Ho claimed he violated none of them. He complained that the deactivation has seriously impacted his social movement campaigns. A Taiwanese political Facebook fan page "Xien Ma Tong" was also disabled and reactivated on the same day. The fan page was created to ridicule the Taiwan president Ma Ying-jeou. Another Facebook fan page "New Taiwan GoGoGO" which relates to a Taiwanese television station also reported that the messages could no be posted though the page was still being there on Facebook. Liu Jian-Kuo, a legislator from the Democratic Progress Party also said his Facebook account was suspended without any warning from Facebook. Taipei City Councilor Ho Zhi-Wei has written an official statement to Facebook, expressing his concern over Facebook's unreasonable account deactivation which has resulted in hindrance to free speech. Global Voices co-founder Rebecca MacKinnon has communicated with executives at Facebook, requesting an explanation of the deactivation incidents in Hong Kong and Taiwan. They say that these incidents were due to a global technical problem that has since been fixed." (Weiping Li 2012).

6.2.7.2 Recent Government Intervention

The recent revolutions in Egypt and Tunisia, and their potential domino effect, were of no small concern to the Chinese government, which promptly took measures to restrict the possibilities of Chinese citizens to obtain news of the events unfolding in the Middle East, banning every item of news referring to those events from the Chinese network.

In August 2010, China's official press agency, Xinhua, and the country's largest state telecommunications operator, China Mobile, signed an agreement to create a joint venture (Search Engine New Media International Communications Co) aimed at launching a search engine directly controlled by the state; in this way the government would be ideally positioned not only to exert even more control over the Internet in China, but also to take advantage of the boom in mobile telephone communications.

Another of the government's objectives in recent years has been its crusade against web anonymity. in 2010, the Chinese Ministry of Technology announced a series of new, restrictive rules for the personal identification of anyone desiring to create a website, and declared all VoIP systems to be illegal.[134]

Internet users must always register prior to posting comments or intervening in any way, although generally the use of pseudonyms is permitted. Since May 2011, however, a new identity authentication system for online news or commercial site forums was introduced, effectively ending anonymous posting on such sites; according to government officials, there are plans to extend this system to all forums and chatrooms as well.

In May 2009 the Ministry of Industry and Information Technology (MIIT) sent notification to computer producers[135] communicating the mandatory pre-installation of a filter software program called in all new computers "Green Dam Youth Escort"; the motivation given was to filter harmful pornographic content and to prevent children from coming into contact with such materials, thus "favoring a healthy and harmonious development" of the Internet. However, ONI researchers who conducted the first analyses[136] demonstrated that the Green Dam software in fact filtered not only pornographic content but also political and religious content generally targeted by China "Great Firewall".

---

[134] See http://digicha.com/index.php/2010/12/chinas-miit-declares-most-voip-services-including-skype-illegal/

[135] See "Notice Regarding the Pre-Installation of "Green" Online Filtering Software on Computers", Ministry of Industry and Information Technology Notice No. 226 [2009], May 19, 2009, http://tech.sina.com.cn/it/2009-06-09/17073163327.shtml., unofficial translation at http://www.hrichina.org/public/contents/press?revision_id=169834&item_id=169820; Xinhua News Agency, "Anti-porn filter software stirs up disputes in China," June 11, 2009, http://news.xinhuanet.com/english/2009-06/11/content_11522822.htm.

[136] See ONI Bullettin, "China's Green Dam: The Implications of Government Control Encroaching on the Home PC", June 12, 2009, http://opennet.net/chinas-green-dam-the-implications-government-control-enchroaching-home-pc.

The new was picked up by international media, resulting in universal condemnation of the regime, which subsequently withdrew the blanket directive. The software is however still mandatory in schools and Internet cafés.

In any case, the Green Dam project represents an episode that is completely without precedent worldwide, of a systematic and totalitarian attempt to move censorship from the national backbone to the private computers belonging to individual citizens, and is even more serious given the many government assurances to its populace that the system was prompted merely by the desire on part of the government to provide computer buyers with a secure, technologically advanced product.

Mobile telephone is not spared these measures, either. A new regulation which came into effect on 1 September 2010 requires prepaid SIM card purchasers to provide identification; those not doing so have 3 years to provide it. Sellers are required to retain copies of all client identity documents.

The Ministry of Industry and Information Technology has explained that the rationale behind this measure is to combat spam and fraud; in reality, however, it is quite evident that it is simply yet a another attempt to tighten the grip of control over users of these technologies, allowing authorities not only to monitor telephone calls, SMS, and data exchanges, but also to easily identify anyone who may distribute or exchange data considered to unacceptable.

6.2.7.3 Legal and Regulatory Frameworks

Despite the fact the Chinese Constitution[137] formally guarantees not only both the freedom of expression and the freedom of the press (Article 35),[138] but also the respect human rights (Article 33),[139] the laws and administrative regulations assure the Chinese Communist Party rigid control over every form of online communication.

The Internet has been closely regulated ever since it first become commercially available in China. In 1994, in fact, the "Regulations of the People's Republic of China for the Safety Protection of Computer Information Systems"[140] granted the Ministry of Public Security the power to "supervise, inspect and guide the security protection work", "investigate and prosecute illegal criminal cases" and to "perform other supervising duties".[141]

---

[137] See http://www.gov.cn/english/2005-08/05/content_20813.htm

[138] **See Article 35** Citizens of the People's Republic of China enjoy freedom of speech, of the press, of assembly, of association, of procession and of demonstration.

[139] **See Article 33** All persons holding the nationality of the People's Republic of China are citizens of the People's Republic of China. All citizens of the People's Republic of China are equal before the law. The state respects and guarantees human rights. Every citizen is entitled to the rights and at the same time must perform the duties prescribed by the Constitution and the law.

[140] Issued by the State Council 18 February 1994.

[141] Art. 17 "Regulations of the People's Republic of China for the Safety Protection of Computer Information Systems", del 18/02/1994.

In February 1996, the State Council issued rules regulating connections between the Chinese domestic network and the international web,[142] placing some of the responsibilities of the control of Internet content to communications companies, essentially obliging them to take over in the implementation of national security objectives.[143]

In 1997 the Ministry of Public Security issued the "Computer Information Network and Internet Security, Protection and Management Regulation",[144] Article 5 of which expressly establishes that it is prohibited to utilize the Internet "to create, replicate, retrieve, or transmit" information for a number of diverse ends, all harmful to the state, including but not limited to "inciting to overthrow the government or the socialist system", "making falsehoods or distorting the truth, spreading rumors, destroying the order of society", e " injuring the reputation of state organs".[145] This regulation confirmed telecommunications companies' obligations, which "must accept the security supervision, inspection, and guidance of the Public Security organization" and assist "the Public Security organization to discover and properly handle incidents involving law violations and criminal activities related to computer information networks".[146]

Every new regulation is, at least officially, based on the attempt to ban to creation or distribution of Internet content deemed "harmful".

---

[142] PRC Interim Regulations Governing the Management of International Computer Networks, February 12, 1996, issued by State Council Order No.195, signed by Premier Li Peng on February 1, 1996.

[143] Article 11: "Units providing international inward and outward channels and interactive and interfacing units shall establish a network management center to strengthen the management of their own units and their consumers according to the relevant laws and state regulation, to improve network information security management, and to provide good and safe services to consumers." Article 13: "Units and individuals engaging in Internet business shall strictly enforce safety and security control systems according to relevant state laws and administrative regulations, and shall not make use of the Internet to conduct criminal activities – including activities prejudicial to state security and the leakage of state secrets – or to produce, retrieve, duplicate, and disseminate information prejudicial to public order or pornographic materials."

[144] Measures of the PRC Regulations for the Safety Protection of Computer Information Systems, cit.

[145] Art. 5: No unit or individual may use the Internet to create, replicate, retrieve, or transmit the following kinds of information: 1. Inciting to resist or violate the Constitution or laws or the implementation of administrative regulations; 2. Inciting to overthrow the government or the socialist system; 3. Inciting division of the country, harming national unification; 4. Inciting hatred or discrimination among nationalities or harming the unity of the nationalities; 5. Making falsehoods or distorting the truth, spreading rumors, destroying the order of society; 6. Promoting feudal superstitions, sexually suggestive material, gambling, violence, murder, 7. Engaging in terrorism or inciting others to criminal activity; openly insulting other people or distorting the truth to slander people; 8. Injuring the reputation of state organs; Other activities against the Constitution, laws or administrative regulations.

[146] Art. 8 Units and individuals engaged in Internet business must accept the security supervision, inspection, and guidance of the Public Security organization. This includes providing to the Public Security organization information, materials and digital document, and assisting the Public Security organization to discover and properly handle incidents involving law violations and criminal activities related to computer information networks.

The most important regulations governing forbidden behaviors are contained to two laws, both issued by the State Council and in effect since 25 September 2000, the "Telecommunications Regulations of the People's Republic of China"[147] and the "Measures for Managing the Internet Information Services".[148]

An analysis of more recent Internet Regulations reveals that Chinese citizens may not create or distribute nine types of internet content: violating the basic principles as they are confirmed in the Constitution; endangering state security, divulging state secrets, subverting the national regime, or jeopardizing the integrity of national unity; harming national honor or interests; inciting hatred against peoples, racism against peoples, or disrupting the solidarity of peoples; disrupting national policies on religion, propagating evil cults and feudal superstitions; spreading rumors, disturbing social order, or disrupting social stability; spreading obscenity, pornography, gambling, violence, terror, or abetting the commission of a crime; insulting or defaming third parties, infringing on legal rights and interests of third parties; other content prohibited by law and administrative regulations.

Two further categories of forbidden behaviors were added by Article 19 of the "Provisions on the Administration of Internet News Information Services" (Internet News Information Services Regulations)[149]:

1. inciting illegal assemblies, associations, marches, demonstrations, or gatherings that disturb social order;
2. conducting activities in the name of an illegal civil organization.

All such behavior may be considered subversive and may lead to fines and criminal liability.[150]

Moreover, the "Measures for Managing the Internet Information Services" cited above establish that ISPs are liable for all content they may render accessible; among the various provisions, Articles 14 and 16 may easily be used to erode the freedom of expression.[151]

---

[147] PRC Telecommunications Regulations, October 11, 2000, issued by State Council Order No.291, signed by Premier Zhu Rongji on September 25, 2000.

[148] Measures for Managing Internet Information Services, issued by State Council Order No.292; signed by Premier Zhu Rongji on September 25, 2000.

[149] "Provisions on the Administration of Internet News Information Services" (Internet News Information Services Regulations) promulgated by the State Council Information Office and the Ministry of Information Industry on September 25, 2005. In inglese all'URL: http://www.cecc.gov/pages/virtualAcad/index.phpd?showsingle=24396.

[150] See, for example, Rules of the NPC Standing Committee on Safeguarding Internet Security, issued by the NPC Standing Committee on December 28, 2000.

[151] See Art. 14: An IIS providing services related to information, the publishing business, and e-announcements shall record the content of the information, the time that the information is released, and the address or the domain name of the Web site. An Internet service provider (ISP) must record such information as the time that its subscribers accessed the Internet, the subscribers' account numbers, the addresses or domain names of the Web sites, and the main telephone numbers they use.

In addition to laws and regulations dedicated to the detection and deletion of any and all unacceptable content, the government has developed a complex strategy to manage and control online media.

Every organization transmitting electronic content relating to politics, the economy and other public affairs must abide by the 2005 "Provisions on the Administration of Internet News Information Services (Internet News Regulations)", already mentioned above; this regulation introduces a system of rules and regulations[152] that is so complex that the *de facto* result is that only state-controlled agencies may distribute online news.

Further rules regarding operator liability are included in the "State Secrets Protection Regulations For Computer Information Systems On The Internet"[153]; on 29 April 2010 an amendment to the State Secret Law obliges companies operating in the Internet and telecommunications sectors to cooperate with authorities for the achievement of national security objectives. Such companies are thus required to block the transmission of undefined "state secrets" on their networks and to alert authorities of every possible violation, and must additionally remove certain content; any violation may result in fines, criminal liability, and even the revocation of the company operating license.

The provisions of China's traditional Criminal Code are used to incriminate electronic dissidents. The measure most frequently invoked is Article 105, incitement to the subversion of the powers of state.[154]

An IIS provider and the ISP must keep a copy of their records for 60 days and furnish them to the relevant state authorities upon demand in accordance with the law. Art. 15: IIS providers shall not produce, reproduce, release, or disseminate information that contains any of the following: 1. Information that goes against the basic principles set in the constitution; 2. Information that endangers national security, divulges state secrets, subverts the government, or undermines national unity; 3. Information that is detrimental to the honor and interests of the state; 4. Information that instigates ethnic hatred or ethnic discrimination, or that undermines national unity; 5. Information that undermines the state's policy towards religions, or that preaches the teachings of evil cults or that promotes feudalistic and superstitious beliefs; 6. Information that disseminates rumors, disturbs social order, or undermines social stability; 7. Information that spreads pornography or other salacious materials; promotes gambling, violence, homicide, or terrorism; or instigates crimes; 8. Information that insults or slanders other people, or infringes upon other people's legitimate rights and interests; or 9. Other information prohibited by the law or administrative regulations. Art.16: When an IIS provider discovers that the information its Web site provides is clearly of a type listed under Article 15, it should immediately stop transmission, keep the relevant records, and report the situation to the relevant state authorities.

[152] See Articles 2, 11 e 15: http://www.cecc.gov/pages/virtualAcad/index.phpd?showsingle=24396.

[153] "State Secrets Protection Regulations For Computer Information Systems On The Internet" issued by the Bureau for the Protection of State Secrets (State Secrets Bureau) on January 25, 2001 but applied retroactively from January 1, 2000. V. in particolare artt. 8, 10 13 e 15.

[154] See Art. 105, par. 2, 1997 Criminal Code: "Anyone who uses rumor, slander or other means to encourage subversion of the political power of the state or to overthrow the socialist system, shall be sentenced to fixed term imprisonment of not more than five years." English language text: www.archieve.org/details/cu31924077027237

Thus the legal apparatus governing the Internet is complex and multifaceted, sustained and implemented by a structural network of controlling authorities and by surveillance strategies that together render the "Great Firewall" the world's most efficient, and most terrifying, control systems.

6.2.7.4 The Role of Foreign Companies in Chinese Censorship

The ethical and political problem inherent to the sale by western Internet filter software producers to eastern states that use those programs to implement censorship campaigns, in clear violation of the human rights of the citizens of the countries in question, has for some time been raised by the international legal community[155] and by international organizations, and was the focus of a recent and excellently researched ONI analysis entitled "*West censoring East: The use of western technologies by Middle East Censors*".[156]

In China this problem is particularly relevant, given that diverse companies (including sector colossals such as Google, Microsoft, Yahoo and Cisco, but also a number of emerging corporations from neighboring countries) are attracted by China's considerable market potentials, and, in order not to risk the loss of the operating licenses that permit them, according to the conditions established by the law and regulations outlined above, to operate in the country, acquiesce to the requests of the government. In some cases these corporations have been sued by Chinese citizens for having contributed to the arrest of dissidents and for having violated their human rights. In a fairly recent case (May 2011), Cisco was sued by the Washington D.C. based Human Rights Law Foundation di Washington in the Federal District Court of San Jose, California for having provided the Chinese government with technology that was clearly to be used for the purpose of repression.[157]

The Google case represented the first exception to this widespread behavior, and focused international public attention on the issue.

The episode began with Google's announcement that it would no longer adhere to the Chinese government's censorship policies, which, as seen above, often affect services offered by search engines. In March 2010 Google in fact declared that Chinese users would be redirected from the Chinese Google homepage google.cn to its homepage in Hong Kong, google.com.hk, where they have access to uncensored content on a version created especially for them. This followed political censorship

[155] See "Corporate Complicity in Internet Censorship in China: Who Cares For The Global Compact or The Global Online Freedom Act?", Surya Deva, in Geo. Wash. Int'l L. Rev., 255 (2007).

[156] See http://opennet.net/west-censoring-east-the-use-western-technologies-middle-east-censors-2010-2011

[157] See www.eff.org/deeplinks/2011/08cisco-and-abuses-human-rights-china-part-1

by Chinese authorities and cyber-attacks against Gmail[158] accounts belonging to a number of Chinese human rights activists and political dissidents.

The case was positive in that it activated international debate on the issue, but Internet censorship remains a complex matter that has yet to be resolve.

The hope for the future is that these corporations, and the numerous other private enterprises that in a variety of ways, through commercial collaboration with repressive governments worldwide, negatively effect the human rights of millions of individuals, work toward the adoption of policies protecting digital liberties and the rights of their users.

Clearly, the decisions of what may circulate in Internet, and what may not, should not be taken by private enterprise nor by a government, but rather by a judiciary authority or any objective third party, impartial to the outcome of the controversy between the parties, and it is of course fundamental that in any case there be the possibility to appeal any decision to remove content.

It would also be highly opportune to create international guidelines that openly confront the ethical issues inherent to the sale of products to government that intend to use those same products against the rights and freedoms of their citizens.

Given the impossibility of embarking upon technological embargos against countries that are, for the most part, still developing, and that so urgently require modern technological infrastructures in order to foster their economies and to expedite their journeys toward democracy.

In 2012, an interesting Article by Rebecca MacKinnon (MacKinnon 2012) analysed the "Google case" after some events that changed a bit the landscape in China. The Authors states that: (i) there is a "ridiculous level of censorship" which "is the work of China's national network-level censorship system that is has been configured to block all Google searches containing words that could potentially be used in politically sensitive contexts" (MacKinnon 2012); (ii) "Google's relationship with China's censors has always been rocky. It is likely to hit a new rough patch after the

[158] Attacks to gMail account (especially) from China are a serious problem. As Weissman notes: "Google has announced, via their security blog, that they will now alert Gmail users if the company believes that a state-sanctioned cyber attack is being directed against them. Google explains that they believe it is their duty 'to be proactive in notifying users about attacks or potential attacks so that they can take action to protect their information'." When suspicious activity arises, Google will notify users with a pink band at the top of the Gmail window that states: 'We believe state-sponsored attackers may be attempting to compromise your account or computer. Protect yourself now.' Although Google refused to say whether this change was directed at any countries in particular, news organizations have previously accused Chinese hackers of using these kind of attacks against the US and other foreign organizations. Additionally, this new alert closely followed a revision to Google's Chinese search that informs users as to whether their search terms are likely to lead to filtering. These new features represent the latest evolution in Google's on-going struggle to provide service in China without becoming totally complicit in China's censorship program. An example of their tête-à-tête includes when Google in 2010 redirected Chinese users to its Hong Kong site, "citing concerns over censorship and hacking." (Weissman 2012).

company rolled out a new feature in 2012 that warns Chinese users when they type words that are known to set off their government's censorship system (MacKinnon report the alert/pop-up message: "We've observed that searching for [the character for river] in mainland China may temporarily break your connection to Google. This interruption is outside of Google's control") (MacKinnon 2012); (iii) "for the first time, Google is making it crystal clear to Chinese Internet users that their frequent connection problems while using its search engine are caused by the Chinese government, not by its own systems" (MacKinnon 2012).

6.2.7.5 Violations of Users' Rights. Digital Resistance and Dissidents in China

Constitutional guarantees are not sufficient to protect those accused by the regime of having committed the actions described above. The judiciary is not independent, and in cases involving the freedom of expression against the regime, even basic procedural guarantees are often not respected. The laws and regulations described above are often utilized to imprison citizens for their online activities, such as posting criticism of the regime or news of human rights violations and the transmission, creation, consultation or downloading of unacceptable content.

The most widely-known case is without a doubt that of Liu Xiaobo, the dissident and intellectual sentenced in December 2009 to 11 years of prison for "inciting subversion of state power" after having distributed online a document he wrote, *Charter 08*, calling for the protection of human rights, political reform and an independent judiciary.

The activist Huang Qi was sentenced, in November of 2009, to 3 years of prison for "possessing state secrets" after having published online criticism of the government rescue efforts following the 2008 earthquake.

In December 2008 Zhao Lianhai, whose son became ill due to contaminated powdered milk, was arrested and accused of "inciting social disorder" for having created an Internet site supporting the families of other children involved.

These are only a few examples of the countless journalists, activists, bloggers, and ethnic and religious minorities sentenced to prison or to work-camps, only a few examples of how laws are often applied not only harshly but also harshly.

In such a repressive climate, individuals seeking to circumvent censorship measures must use all their ingenuity.

Among the various techniques utilized in countries governed by totalitarian regimes, one developed in China deserved particular mention.

The Chinese are some of the most devoted and expert videogame players in the world, and the Chinese language is full of homophones, many of which may be used for word games and double entendres.

For years, Chinese netizens have amused themselves by making fun of their censors through the use of these word games, creating fantasy characters, who are often then transposed to videogames. In this context then, the battle against censorship is represented by a mythical creature called Caomina, a "grass-mud horse", which is the

homonym of a common insult in Chinese. The imagination of Chinese netizens has no limits, inventing false reports, songs, video, and untold other material involving the grass-mud horse, and creating figures and characters that represent the regime.

The ingenuity and imagination of the Chinese people thus allow them to lighten, even if only for a moments at a time, a battle that they, and the entire world, must win. This does not change the fact that this particular topic, involves the protection and respect of human rights, is of fundamental importance and requires rapid resolution.

6.2.8 Turkmenistan: Censorship and Control

6.2.8.1 Main Issues

Turkmenistan has been an independent state in Asia since 1991, following the breakup of the Soviet Union. Since gaining independence, however, the state has always had an authoritarian regime. The country's first President, Saparmurat Niyazov, was proclaimed "President for Life" and granted absolute powers.

In 2006 the President was felled by a heart attack, and was succeeded by the current President Gurbanguly Berdimuhammedow, who, from the beginning of his term, has consistently maintained that he plans to allow the country to evolve and to introduce democratic reform, although thus far results have been decidedly few.[159]

All media are completely under government control, and the Internet penetration rate is one of the lowest in world, only 1.4% of the country's population.

This is due to excessively high costs and to a dearth of Internet cafés, with very slow connection speeds and costs so high as to render web access a luxury for an elite few.

The Constitution, which has been revised several times, is the most important source for the country's legal and regulatory system. A new version of the Constitution, approved in 2008, is currently in force. It makes reference to liberal principles,[160] expressly granting the citizens of Turkmenistan the freedoms of speech and expressions.

The actual situation, however, is quite different. An even cursory analysis of the nation's laws quickly reveals numerous limitations to the freedom of expression, with laws whose criteria are extremely vague and arbitrary.

---

[159] See http://www.icnl.org/knowledge/ngolawmonitor/turkmenistan.htm.

[160] The text of Article 23: "Article 23: Every citizen has the right to be protected from arbitrary interference in her or his personal life, from infringement on written, telephone, or other communications, and, likewise, from infringements on her or his honor or reputation." The text of Article 26 is: "Article 26: Citizens of Turkmenistan have the right to freedom of conviction and the free expression of those convictions. They also have the right to receive information unless such information is a governmental, official, or commercial secret."

Perhaps most dangerous for Turkmen citizens are the numerous offenses listed in the country's criminal code that are plainly crimes of opinion, and in particular Article 133, which punishes any insult to government agents with a fine, or 2 years of forced labor, or 1 year of imprisonment, and Article 132 which allocates similar punishments for defamation or libel utilizing any mass media platform. Offenses against the President carry much harsher sanctions. Any attempt against his life or health may be punishable with a life sentence or the death penalty, while libel directed against the President may result in a prison sentence of up to 5 years.

However, these laws, which in and of themselves are nothing extraordinary, and are found in many modern legal systems, must, in order to fully understand their full breadth, be interpreted in the context of Turkmenistan's Law on Terrorism.[161]

Taken together, these pieces of legislation have created a system of global censorship and have imposed total self-censorship on nearly all aspects of Turkmen society, not only those relating to terrorist movements, but also relating to any opposition to government policy or even members of the government, conferring upon the executive branch wide – it would probably not be going too far to say virtually unlimited – coordination and intervention powers that may be implemented at even the suggestion of terrorist activity, the definition of which is deemed to be any activity against the state.

The universality of the environment of the application of the law is rendered even more vague by the an express reference in Article 2, in which it is established that essentially all the country's legal sources, in addition to all international principles in force, are to be considered the "basis" for the anti-terrorism law.

The ramifications are twofold:

1. This Law is, given its wording, extremely flexible, easy to modify and adaptable to nearly any case or situation, and is thus in clear contrast to the legal principle of the certainty of law;
2. the sweeping powers of surveillance and censorship granted to authorities are completely quite applicable even in the total absence of any suspicion of terrorism.

With the addition of the portion dedicated to the freedom of speech, Article 11 of the Law on Terrorism, entitled "The Role of Public Associations and the Mass Media in Combatting Terrorism", the breadth of the application of this law become truly unlimited, imposed on every association and above all on the media in order to avoid any content that might in any way conflict with the "*high spiritual-moral ideals, at forming with the young generation the feeling of national pride, devotion towards people's traditions, towards the nation, readiness to sacrifice life for the sake of the beloved Motherland, for its safety and integrity*".

In other words, in addition to a law that may be nearly universally applied by authorities to nearly any situation, there is also a criteria of constant and total self-censorship that is so generic, and so lacking in any objective elements, that nearly any activity that does not please the government may be classified as subversive.

[161] See http://turkmeniya.tripod.com/turkmenistanlaws/id13.html

In conclusion, the Turkmen legal framework appears to oppose every basic principle of modern law.

6.2.8.2 Internet Access and Filtering systems

The legislative scenario described above and the complete control of the country's entire media system by the state render freedom of speech nearly inexistent in Turkmenistan.

As mentioned at the beginning of this section, internet is largely unavailable because of its high costs. Currently domestic Internet connections involve fees that are prohibitively high even by western standards and much more so in a country in dire economic conditions.

Today the only other way to access Internet in Turkmenistan is to use the connections available in the country's few luxury hotels, but here, too the costs involved are far too high for the average citizen.

Until 2006 there were no Internet cafés in the country, but after the death of the first President, his successor, Berdymukhamedov, decided to pursue a new era of freedom. In reality, however, his first disposition, with which he created two Internet cafés in the country's capital, also included a number of elements bordering on the surreal; not least of which was the fact that once they were finally opened, clients had to pass by two soldiers placed at the entrance of each, placed there to monitor their "correct use". More recently, however, the President has authorized the opening of additional cafés in the capital and in the country's principal cities, bringing the total number to just over a dozen.

The low Internet use levels make it very easy for the government to conduct pervasive filtering of the few users who do connect to the Internet, especially given the fact that the country's only ISP is run by the state owned TurkmenTelekom.

On a purely formal the presence in the Turkmen market of private ISPs is a possibility, but it is nearly impossible to obtain an operating license from the authorities in Ashgabat. To date there has been only one case, That of the provider Ariana, whose license was revoked after only a few months of having been granted.

It is also obvious, in a system such as that of the Turkmenistan, that very few companies seek to invest in the country's Internet system, which in addition to being extremely complex, is also so very limited.

All connections in the country pass the TurkmenTelecom's central hub, where are thoroughly monitored and checked for blacklisted keywords (which include the name of the President). Given the limited availability of internet and the presence of a single provider, filtering and monitoring are particularly severe.

TurkmenTelecom places a number of significant limits to the use of internet connections.

Firstly, in order to obtain a user account, it is necessary to register, using a valid passport. When registering, users are informed of the following prohibitions:

1. posting materials containing foul language, showing "inappropriate behavior online, posting information that conflicts with the standard norms of behavior and legislation, and uploading pornographic materials",

2. making or distributing "untruthful and defamatory information", and
3. any action against the state. In the event of any violation, the provider, in addition to any criminal sanctions that might be applicable, is authorized to rescind the contract.

The state imposes significant self-censure on foreign organizations and the few luxury hotels able to afford the high cost of internet connections, filtering all sites supporting the opposition. Internet is becoming increasingly available in the country's schools, but the filtering system is so extended that connections so slow as to be nearly unusable.

There are currently very few Turkmen Internet sites. Nonetheless, their number is slowly growing, although registration costs are quite high, for a very simple reason, the suffix utilized by the country is .tm, the same domain for TradeMark, which for obvious reasons is quite sought after by companies worldwide.

In addition to a sole provider, nearly non-existent Internet penetration, and pervasive content filtering, the state has additionally blacklisted numerous sites that are thus impossible to access from within Turkmenistan; these include sites regarding freedom of expression, religious freedom and any site opposing any aspect of Turkmen government policy.

Turkmenistan is in fact considered by numerous humanitarian associations to be one of the states with the most widely developed systems for censorship and repression.

Reports available on the Internet feature numerous cases of the persecution of journalists, torture, and diverse cases of mysterious deaths.

Turkmenistan Helsinki Foundation[162] is a humanitarian association headquartered in Varna (Bulgaria), which is quite active in promoting human rights and the freedom of expression Turkmenistan. Two of its members are currently detained in a Turkmen prison.

Additionally, as of the present writing, there are numerous individuals behind bars for crimes of opinion, and, in general, the situations regarding human rights is extremely grave.

The current President on numerous occasions has demonstrated that he wishes to change the direction of his country, which has the potential to become quite wealthy given its significant reserves of natural and petroleum. However, to date very little indeed has been accomplished.

6.2.9 Uzbekistan: Internet, Censorship and Surveillance

6.2.9.1 The Internet Presence in the Country

Uzbekistan has been an independent state since 1991, following the breakup of the Soviet Union. While the laws passed in this fledgling state would certainly seem to

[162] See http://www.tmhelsinki.org/en/

reflect a democratic spirit, the facts and events since the country's independence cause Uzbekistan's government to be considered, by many scholars, far from liberal, with shades of absolutism. In the 20 years since gaining its sovereignty, the country has had the same President (appointed leader even before the country's independence by the Kremlin) and virtually all political parties participating in government (while formally diverse) in fact give complete support to this single figure. Moreover, nearly all legislative and decisional power within the country lies exclusively with the executive branch and particularly with the President (whose power is thus practically unlimited), leaving very little space for any democratic expression whatsoever. The Uzbek State has progressively taken on a key geopolitical role in the area between the ex-USSR and the Far East, due among other factors to considerable demographic growth during the course of the last century.

During the same period, the country's mass media enjoyed similar growth, despite the fact that, until 1995, Internet was not present in the country. From its first availability, the diffusion of Internet within the country has continued to grow exponentially based on recent statistics,[163] 26.8% of the population in Uzbekistan now has access to Internet, while in 2006 this figure was only at 6.45%. It is however important to underline that domestic connections still carry costs that are prohibitive for the majority of the population, with the consequent diffusion of Internet cafés. This increase in the number of connections and the ability to connect to the Internet have not, however, resulted in any parallel increase in Internet freedom, with connections continuing to be extensively limited by an oppressive system of bureaucratic and administrative regulations and by a highly repressive legal system.[164]

6.2.9.2 The Legal and Regulatory Framework

At least formally, freedoms of speech and of expression are strongly protected by the Uzbek legal framework. The primary source of these protections is the Constitution,[165] ratified in 1992, which dedicates three Articles to the freedom of

[163] See *Internet World Stats* (Uzbekistan) at the address http://www.internetworldstats.com/asia/uz.htm. Accessed 24 October 2011.

[164] In 2011, the authors of an *Internet Enemies Report*, edited by *Reporters Without Borders, at the address* http://12mars.rsf.org/i/Internet_Enemies.pdf (accessed 24 October 2011) commented (italics mine): "Despite the European Union's decision in late 2009 to lift the sanctions against Uzbekistan, the regime *has not loosened its grasp on the Net* – quite the contrary. This police state is still routinely *preventing the dissemination of information online and all efforts to initiate a civil society* – virtual or any other kind". (RWB Report 2011: 46).

[165] For a plain overview of constitutional issues, see the Niyazova report concerning the substantial absence of free and independent media and of free speech in Uzbekistan (Niyazova 2008). The author notes: "It is noted that, in violation of its constitutional and international obligations in the field of human rights, the government of Uzbekistan prevents the dissemination of any information that is critical of the government and exerts pressure on journalists and individual citizens in the community". (Niyazova 2008: 1).

speech, Article 25[166] and 29,[167] which guarantee the freedom of "thought, speech and convictions", and Article 67,[168] regulating the country's mass media system, which, among other things, expressly prohibits all forms of censorship ("Censorship is impermissible").

Article 29, particularly, prohibits anyone from seeking, obtaining and disseminating any information directed against the existing constitutional system, or divulging any State secret or confidential corporate information. Notice, also, that Article 30 obligates state bodies, public officials and public associations to "allow any citizen access to documents, resolutions and other materials, relating to their rights and interests", and Article 43 provides that the State "shall safeguard the rights and freedoms of citizens proclaimed by the Constitution and laws".

The rest of the Nation's legal system is at least formally inspired by similarly liberal values; however, when analyzed in a more detailed fashion, numerous laws are clearly in marked contrast with these principles.

Recent legislation deserving particular attention includes the *Mass Media Law*, first approved in the 1990s and now in its fourth version, which took effect on January 15, 2007. This Law clearly reflects the state's "*legislativehypocrisy*", with a first portion inspired by democratic and liberal ideals (in which both the freedom of speech and the prohibition of all forms of censorship figure prominently), while the rest of the of the law goes on to establish a series of regulations that are not only extremely restrictive but also completely arbitrary.[169]

---

[166] The text of Article 25 of the Uzbek Constitution is: "Everyone shall have the right to freedom and inviolability of the person. No one may be arrested or taken into custody except on lawful grounds". http://www.gov.uz/en/constitution/. Accessed 23 October 2011.

[167] The text of Article 29 of the Uzbek Constitution is: "Everyone shall be guaranteed freedom of thought, speech and convictions. Everyone shall have the right to seek, obtain and disseminate any information, except that which is directed against the existing constitutional system and in some other instances specified by law". http://www.gov.uz/en/constitution/. Accessed 23 October 2011.

[168] The text of Article 67 of the Uzbek Constitution is: "The mass media shall be free and act in accordance with the law. It shall bear responsibility for trustworthiness of information in a prescribed manner. Censorship is impermissible". http://www.gov.uz/en/constitution/. Accessed 23 October 2011.

[169] In 2011 the authors of the *Internet Enemies Report*, cited above, edited by *Reporters Without Borders, at the address* http://12mars.rsf.org/i/Internet_Enemies.pdf (accessed 24 October 2011) commented: "The Centre for Monitoring Mass Communications (CMMC) closely monitors the content of Internet websites and audiovisual media. Reporting to the Uzbek Agency for Communications and Information (UzASCI), it is responsible for blocking the IP addresses of the sites or articles which it deems undesirable. […] Sensitive subjects include criticism of the government, information on the actual state of the economy, human rights and the social situation. It is not advisable to discuss the private business of the Karimov family or their daughters' personal lives, the forced labour of children in cotton fields, or emergency situations. It is much too risky to mention petrol supply problems, inflation, the population's impoverishment, and social unrest. Any reference to the Andijan massacre is simply removed. The population has long since stopped bringing up the subject in public – and even in private. Self-censorship is widespread" (RWB Report 2011: 46–47).

This law, too, confirms, as does the country's Journalism Law,[170] that the Internet falls within the scope of these mass media laws[171] and is to be regulated accordingly. This has immediate repercussions, given that in this way, not only are all general laws regulating other channels of mass communication, such as television, newspapers and radio deemed applicable to the Internet, but also, and most dangerously, those relating to news and information. Thus even a simple blog is legally subject to all the same requirements obligations and liabilities as a news magazine or journal.

In a 2004 Memorandum by Article 19,[172] concerns about this extension are clear:

> The definition of 'mass media' is extremely broad, apparently reaching virtually every conceivable communication of information, provided only that such communication has a "permanent title". For example, "electronic and digital communication" would appear to include within its reach any form of Internet conveyance of information whatsoever as long as it has some sort of caption which could be counted as a "title". Certainly, this could include small newsletters and other regular and somewhat formalised exchanges of information on the Internet; by terms, it could even apply to individual private emails which contain a subject line. Small print publications by clubs or associations meant solely for their membership would appear to be included, regardless of the size of their print run or circulation – a small bulletin distributed to ten persons, or a flyer distributed on a street corner to passers-by, could be covered. The definition also, of course, covers all the mass media, more regularly understood, including print media and broadcast media. (Article 19 Memorandum 2004: 6).

Upon closer examination of the general regulation of mass media in Uzbekistan, one immediately finds an extremely controversial provision, also included in the law regulating journalists, establishing a number of *preconditions* necessary in order to publish or even communicate news stories. Thus all information reported must not only be true, but must also be reported *with objectivity*. This requirement, which at first glance might appear legitimate, in reality constitutes an evaluation criterion so entirely subjective and arbitrary, so subject to personal opinion, that any piece of news and any publication is always very easily repressed.

In order to fully understand the breadth of this piece of legislation, it might be useful to consider it together with the *Media Law*, and specifically with Article 6, which imposes a series of limits to freedom of speech, authorizing censorship for

[170] "Law on protecting the professional activities of the journalist", dated 24 April 1997.

[171] See Article 1 of the law (italics mine) including electronic information media: "The mass media are newspapers, magazines, journals, bulletins, news agencies, television (including cable, and broadcasting and cable television) and radio stations, documentary films, *electronic information media*, and other mass state and independent periodicals, which are published under a permanent name" and the explicit provision of Article 4 of the Law: "websites in generally-accessible telecommunications networks are considered media, and their formats have to be registered".

[172] Article 19. 2004. Memorandum on the Law of the Republic of Uzbekistan on Mass Media. Commissioned by the Representative on Freedom of the Media of the Organisation for Security and Cooperation in Europe. http://www.article19.org/data/files/pdfs/analysis/uzbekistan-law-on-freedom-of-information-June-.pdf. Accessed 24 October 2011.

"propaganda" of any kind for terrorism, extremism, separatism, fundamentalism and pornography. It is quite clear that the range of this law renders it ideal for prohibiting nearly any sort of content whatsoever. The targets of these requirements are ISPs, web site administrators, authors of online publications, and, for news sites, journalists and their editors.

Governmental authorities, in the event any aspect of these strict limits are not fully respected, have an extremely wide breadth of intervention, having the authority to suspend, block and shut down sites, with no other motivation needed than a very general "violation of the law" and may even based on the mere technical non-conformity of the site (Article 24). The State, in order to better verify full observance of this law, requires all media (and therefore also on internet sites and blogs) to register with authorities (Articles 13 and following, *Media Law*), rendering any web anonymity simply impossible.

The abovementioned 2004 Memorandum by Article 19 expresses concerns with regard to this law:

> For one thing, it attempts to regulate in a single set of broad provisions all aspects and fields of mass media even though, as we detail below, very different regimes are needed to regulate, for example, the broadcast media and the print media. In addition, certain publication activities which the Law currently does regulate, such as the activities of small Internet publishers and the informal activities of non-governmental organisations, should not be subject to any regulation at all. Other fundamental difficulties include that the Law imposes a responsibility on the mass media amounting effectively to a prohibition on the publication of "false news"; imposes onerous content restrictions on the publication of materials, as well as obtrusive registration requirements, the latter wielded by an "authorised agency" which is almost certainly not independent of government; imposes an overbroad obligation on the mass media to publish corrections or responses; and gives government and courts the power to command publication of certain materials which is entirely inappropriate. (Article 19 Memorandum 2004: 2).

In general, in addition to the Uzbek Media Law, the Country's legal system is a byzantine maze of laws and regulations, all aiming to create further space for state intervention and to afford the state and its agencies ever wider powers. In fact, a 2002 law relative to the "Principles and Guarantees on Access information" apparently for no other reason that augment the state's decisional and intervention powers, authorized state agencies to carry out any intervention necessary for the protection of individuals "from any information that might have negative psychological influence". Once again, therefore, a criterion that is absolutely subjective, and in clear contrast to legal principles of certainty, a fundamental aspect of all democratic legal systems.

6.2.9.3 State Internet Monitoring and Surveillance Systems and Tools

Accompanying the laws described above, the Uzbek government has created state bodies to enforce them. Over the course of the last decade, numerous agencies and public entities[173] were formed, all having the task of authorizing, managing

[173] For example: Uzinfocom, the agency for the control of technology, UzSCINET, the agency for the academic research, UzCIA, the agency for communication and information, SNB, the agency for the internal security and UzPia, the agency for the press and information.

and successively monitoring all media, and most particularly, Internet activities.[174]

The first of many government checks occurs at the very root level: in order to perform ISP functions in Uzbekistan, in fact, it is obligatory to obtain prior permission, in the form of an operating license, from the UzCia. This license typically lasts for a 10-year period and binds operators to the rigid observance of all laws in effect relative to unauthorized content. The task of surveying the compliance of ISPs with these requirements is left to another state agency, *UzTelecomn*.[175]

With the progressive diffusion of Internet, a new entity, the *National Network of Information Transmission* (UzPAK),[176] to which was entrusted a monopoly of the management of Internet connections, and the suffix .uz for Uzbek Internet sites were created. But UzPAK, as might be imagined, did not limit itself to technically managing connection, but rather performed the first phase of content monitoring, applying a specially created filtering system. As demand for Internet access in Uzbekistan grew, so did the number of service providers, which, however, were rigidly bound to the country's sole Internet exchange point, called "Tas-IX", and is physically located on the premises of the central Post and Telegraph agency.

With Regulation 352 of 2007, UzPak's connection monopoly was eliminated, although 80% of the country's connections continue to be managed by this agency, while the remaining ISPs utilize a satellite connections. The presence of this small group of providers is not, however, at this time sufficient to be considered as providing any real hope for future change. In addition to state entities and agencies created specifically to control the Internet, in fact, in Uzbekistan the Internal Security Agency (SNB), the state intelligence agency, exerts rigid control over all aspects of communication. The SNB in fact performs wide-reaching surveillance and monitoring activities over the Internet and all content, using filtering software as well.

Moreover, the SNB has the autonomous power, as established by Article 24 of the *Mass Media Law*, to intervene directly on websites that it deems noncompliant with the regulation, and to block single pages and even entire sites.

---

[174] In the 2011 *Internet Enemies Report*, cited above, by Reporters Without Borders (http://12mars.rsf.org/i/Internet_Enemies.pdf) observes: "The one thousand or so cybercafés operating in the country are not evenly monitored. There is a widespread use of spyware. Tests conducted by Reporters Without Borders have shown that certain café managers reacted when anti- spyware software was installed on one of their computers, while in other cybercafés, such tampering went unnoticed. Some censorship circumvention tools may have been used in certain cafés, but not in others. Several OpenNet Initiative researchers were questioned in 2007 while they were testing website filtering systems. E-mails are also under surveillance, as are chat rooms, particular those of ICQ and Mail.ru Agent. Several people were supposedly arrested in January 2010 for their alleged membership in extremist religious organisations after they were apprehended based on the content of their chats on Mail. ru Agent". (RWB Report 2011: 48).

[175] According to Regulation n. 221, 2005.

[176] According to Regulation n. 52, 1999.

The SNB, moreover, partially recycling, Soviet customs by which individuals were encouraged to inform on anyone opposing the regime, strongly invites not only ISPs but also Internet cafés to auto-censure all unauthorized content, and to indicate any unapproved use to authorities.

Obviously, should such invitations not be respected, operating licenses in Uzbekistan are very easily (and, based on information available on the web, quite arbitrarily) revoked.

Often censorship of undesired content by the SNB occurs unofficially, with a simple, informal request to the host ISP, which, obviously, cannot take the risk of not following the order.

6.2.9.4 Censorship and Repression

Thus it is clear that censorship in Uzbekistan has reached levels that, to say the least, are quite preoccupying. Causing further concern are the multiple episodes of violent repression by the state, which in the past has never hesitated to resort to violence in order to suppress even peaceful rallies by its citizens. Really cruel was the 2005 Andijian repression.

To date numerous journalist, bloggers and human rights activists have been intimidated or imprisoned and mysterious deaths among the country's dissidents are not uncommon. Among such cases is that of the journalist and human rights activist Umida Niyazova, who in 2007 was arrested and tortured before being released. Another emblematic case is that of Djamshid Karimov, the nephew of the President; Karimov dared to publish a number of articles denouncing state corruption, and in retaliation, in 2006, was interned in a psychiatric hospital, where, to the date of this writing, he remains.

The list of imperiled activists and journalists is, sadly, quite long and numerous Uzbek individuals are currently in prison for the crime of having expressed their opinions.

Based on a number of recent news stories posted to the web, it would appear that Uzbeks are seeking to reform their country's media system, and most specifically the internet. Yet it is difficult to imagine how any real change could be brought about under the present regime.

Concerning web censorship in the country, Niyazova notes:

> The new law defines websites as part of the media. This means that websites come under the law which requires all local and foreign media to apply for registration with the authorities and to report to them the names of the founder, chief editor and all those on the staff. Over the last five years, the country's authorities have systematically blocked access to informative and socio-political web resources. The administrators of every Internet café have to display posters warning the public against visiting banned websites, which include political opposition or foreign websites publishing material about the Central Asian region. At the present time, users have no right of access to several hundred Internet sites. Basically, all the websites of opposition parties and movements, and also most foreign and Russian sites which publish articles throwing light on events in Uzbekistan, are blocked.

> The government has blocked access to Internet sites which publish articles about the murder of the journalist Alisher Saipov, an ethnic Uzbek, who lived in Osh in the Republic of Kyrgyzstan, and was renowned for his critical articles about Uzbekistan. (Niyazova 2008: 4).

6.2.10 Vietnam: Digital Resistance and Censorship

6.2.10.1 Institutions, the Legal Framework and Internet Connection

Vietnam has been an independent country since 2 September 1945, when President Ho Chi Minh read the country's declaration of independence in Saigon's Ba Đình Square. The same day, Ho Chi Minh was elected President of the new Democratic Republic of Vietnam. From that moment on, the nation has been at constant war, both colonial and internal. In later years, the territory was partitioned into two republics (North Vietnam and South Vietnam). The period between 1954 and 1975 saw a number of bloody conflicts, some seeking the reunification of the original state. Perhaps the most violent was the conflict now referred to as "The Vietnam War", and lasted from 1960 to 1975. Once the wars were over, the territory was reunified under the control of the Northern government, with the name of the Socialist Republic of Vietnam. Saigon, the capital, was renamed Ho Chi Minh (the name of the president). However, in the first decade following unification, the country's economy was nearly always in crisis and nearly none of the socio-economic objectives for that period were met. Vietnam has been a member of the WTO (World Trade Organization) since 2006.[177]

The Vietnamese Government[178] and the National Assembly[179] (equivalent to Parliament) are the Republic's institutional bodies. The National Assembly oversees the implementation of the Constitution and laws. It additionally governs the state apparatus in every sphere of Vietnamese life. Within the NA diverse commissions address specific issues. In particular, the Commission for Science, Technology and the Environment vets bills introduced to the NA and implements development policy in the fields of science, technology, ecology and the environment. Additionally the commission may also propose financial policy for the above fields.

The fundamental text for Vietnam's judicial system is the Constitution of the Socialist Republic,[180] adopted on 15 April 1992 and most recently approved by the NA in December 2001.

---

[177] See http://www.chinhphu.vn/portal/page?_pageid=439,40237488&_dad=portal&_schema=PORTAL&pers_id=1093197&item_id=1093699&p_details=1. Accessed 15 November 2011.

[178] See http://www.chinhphu.vn/portal/page?_pageid=598,1&_dad=portal&_schema=PORTAL. Accessed 15 November 2011.

[179] See http://www.na.gov.vn/htx/English/#387gTwKHgoDA. Accessed 15 November 2011.

[180] See http://www.chinhphu.vn/portal/page?_pageid=439,1090502&_dad=portal&_schema=PORTAL. Accessed 15 November 2011.

From 2005 to 2006 the number of Internet users in Vietnam grew exponentially, from approximately 9 to 14.5 million, with a penetration level of 17%. Half of the Vietnamese population is under 30 years old, and a majority frequent cybercafés. According to a 2010 estimate,[181] nearly 26,8 individuals used Internet in Vietnam, equal to 31.11% of the population, and of these over 1.5 million have a blog.[182]

6.2.10.2 The Freedom of Speech in the Constitution and in the Legal System

The Vietnamese Constitution guarantees both the freedom of the press and freedom of speech. The provision containing these guarantees, however, is quite vague and above all does not preclude limitations to these rights. Article 69 of the Constitution, under Title V,[183] called Citizen's Fundamental Rights and Duties, states the following: *The citizen shall enjoy freedom of opinion and speech, freedom of the press, the right to be informed, and the right to assemble, form associations and hold demonstrations in accordance with the provisions of the law.*

Moreover, Article 258 of the country's the Criminal Code[184] establishes prison sentences of up to 3 years (seven in certain circumstances) for the abuse of the exercise of democratic liberties (including those of the freedom the press and the freedom of speech) at the expense of the state and the rights of organizations and individuals: *Those who abuse the rights to freedom of speech, freedom of press, freedom of belief, religion, assembly, association and other democratic freedoms to infringe upon the interests of the State, the legitimate rights and interests of organizations and/or citizens, shall be subject to warning, non-custodial reform for up to three years or a prison term of between six months and three years. Committing the offense in serious circumstances, the offenders shall be sentenced to between two and seven years of imprisonment.*

---

[181] See http://english.mic.gov.vn/vbqppl/Lists/Vn%20bn%20QPPL/AllItems.aspx?curpage=1. Accessed 15 November 2011.

[182] For an overview regarding Internet connection in Vietnam see the Lam, Boymal and Martin essay concerning the techno-economic factors that determine the diffusion of the Internet in Vietnam (Lam et al. 2004). The authors remark that "it should be noted that, in the specific social and political context of the Vietnamese case, gathering relevant materials and statistical data is a very hard and time-consuming task owing to the prevailing culture of 'secrecy' and the scarcity of reliable statistical data and documentation on the topic"(Lam et al. 2004: 42).

[183] Seehttp://www.chinhphu.vn/portal/page?_pageid=439,1096053&_dad=portal&_schema=PORTAL. Accessed 15 November 2011.

[184] See http://moj.gov.vn/vbpq/en/Lists/Vn%20bn%20php%20lut/View_Detail.aspx?ItemID=610. Accessed 15 November 2011. The text of Article 125 is: "Infringement upon other persons privacy or safety of letters, telephone and/or telegraph", the text of Article 225 is: "Breaching regulations on operating, exploiting and using computer networks" and Article 226 "Illegally using information in computer networks".

Decree 56/2006/ND-CP[185] became effective on 1 July 2006, establishing strict sanctions for violations committed in the course of any cultural and information activities. The provisions in question provide for fines of up to 30 million dong (2,000 US dollars) for those who disseminate political party or state secrets. Thus Vietnam's legal framework, including the country's Press Law of 28 December 1989, as modified by Law 12/1999/QH10 of 12 June 1999,[186] over the years has resulted in the imprisonment of not only numerous journalists but also many regular citizens and bloggers. The case of Le Chi Quang is emblematic. He was arrested on 12 February 2002 by police who had surrounded an Internet café in Hanoi to capture him. His home was searched and all his documents confiscated. In November 2002, after a closed hearing of just over 3 h, he was sentenced to 4 years of prison and 3 years of parole for having distributed "propaganda against the Socialist Republic of Vietnam". At the end of August 2011, 17 bloggers and 3 journalists[187] are behind bars for offenses substantially identical to those of Le Chi Quang.

The situation regarding Vietnam's communication infrastructure is equally bleak. The three largest Internet Service Providers are VNPT, which controls 74% of the market and is owned by the state, Viettel, owned by the military and with a market share of 11%, and FPT, the only privately owned ISP (10%). VNPT and Viettel together also possess the three largest mobile telephone companies (MobiFone, VinaPhone e Viettel), with 110 million customers between them. Although Vietnam does not have a legally imposed state monopoly on market access for new providers, a number of informal practices create significant obstacles for new enterprises seeking to enter the Vietnamese telecommunications sector.

The sector is regulated by a law introduced in 2006, Law 67/2006/QH1,[188] known as the Information Technology Law. Article 20, entitled "Monitoring and supervision of digital news content" establishes for content regulation as follows: *Competent state agencies shall monitor and supervise digital information; investigate law violations committed in the course of transmitting or storing digital information. Except when requested by competent state agencies, organizations and individuals engaged in information technology application are neither responsible for monitoring or supervising digital information of other organizations and individuals nor for investigating law violations committed in the course of transmitting or storing digital information of other organizations and individuals.*

In recent years, the Ministry of Science and Technology[189] has invested in information and communication technology in order to revitalize the ICT sector and to increase access to these technologies in Vietnam.[190] *YouTube*, *Twitter* and all international

[185] See http://moj.gov.vn/vbpq/en/Lists/Vn%20bn%20php%20lut/View_Detail.aspx?ItemID=5422

[186] See http://moj.gov.vn/vbpq/en/Lists/Vn%20bn%20php%20lut/View_Detail.aspx?ItemID=918

[187] See http://en.rsf.org/vietnam-eight-bloggers-get-sentences-12-10-2009,34653.html

[188] Seehttp://moj.gov.vn/vbpq/en/Lists/Vn%20bn%20php%20lut/View_Detail.aspx?ItemID=4761. Accessed 15 November 2011.

[189] See http://www.most.gov.vn/. Accessed 15 November 2011.

[190] See http://www.most.gov.vn/Desktop.aspx/Bai-viet-Hoat-Dong-KHCN/Chien-luoc-quy-hoach-ke-hoach/CHIEN_LUOC_QUY_HOACH_KE_HOACH/. Accessed 15 November 2011.

hosting sites are freely accessible and rapidly increasing in popularity, although in 2009, on the order from the Ministry of Public Security,[191] the country's ISPs were obliged to block *Facebook*, that at the time already had nearly one million registered users in Vietnam. The site was only sporadically accessible for the whole of 2010, while the government steadfastly refused to officially admit to the block. However, information on how to evade the blocks and reach *Facebook* despite them circulated over the web. In fact, by the end of 2010 the number of registered *Facebook* in Vietnam had risen to nearly two million, almost doubling in spite of the blocks imposed.

In May 2010 the Ministry of Information and Culture launched its own social network called GoVN,[192] but one in which users must register under their own names and receive a government issued user number in order to create the account and access the network. Initial response to the new initiative has been limited, as might be imagined.

In 2009 the government censored Catholic web sites, especially sites like The VietCatholic News, Catholic News Agency, Catholic Online, Asia News, Catholic World News and Independent Catholic News. Targets were the protests in which Catholics were seeking the return of confiscated church properties.

An interesting Nguyen and Schauder essay regarding e-government in Vietnam (Nguyen and Schauder 2007) examines the capacity of citizens to become effective users of e-government services in terms of their access to, and capacity to use, ICTs and how government in Vietnam might position itself better to provide effective e-government services. The authors remarks that the drive towards effective e-government service delivery needs to be accompanied by a re-examination of government processes, especially in terms of their responsiveness to citizens' needs (Nguyen and Schauder 2007: 50).

Anh Tuân, describing 10 years of electronic media in Vietnam and the activities of VietNamNet (Anh Tuân 2007), remarks that:

> Before the first email was sent from VietNet, the Internet became a deeply contentious political issue. Many senior government officials were deeply suspicious of foreign political and cultural influence. They were afraid that the Internet would be a conduit for the dissemination of subversive ideas. Engineers who did not agree with my Unix and TCP/IP-based approach played into the fears of the leadership. They advocated for Vietnam to develop its own information transfer protocol that was not based on the international standard. Only in this way, they argued, could Vietnam maintain its sovereignty and guard against foreign influence! […] Since VietNamNet was established in 1997, the Vietnamese government's attitude towards the Internet and online media has evolved to one that is perhaps best described as guarded ambivalence. On the one hand, the government recognizes the importance of the Internet as an essential element of the contemporary world […] On the other hand, the suspicion with which some government officials viewed VietNet, while lessened, still remains. Online content is monitored closely and several Internet news

[191] See http://www.chinhphu.vn/portal/page?_pageid=439,1090430&_dad=portal&_schema=PORTAL. Accessed 20 November 2011.

[192] See http://www.go.vn/. Accessed 20 November 2011.

> sites have been penalized for various content-related offenses. It is interesting to note that the government's concerted efforts to monitor Vietnam-based online media outlets do not extend to international news sites […] This is in sharp contrast to China, which maintains an extensive firewall that blocks access to most English-language media. (Anh Tuân 2007: 8, 9, 18, 19).

6.2.11 Australia: Internet Filtering Policies, Digital Liberties and Circumvention Tools

6.2.11.1 The Political Framework

Australia is a constitutional monarchy with a federal division of powers, whose head of state is the ruler of Great Britain, Queen Elizabeth II. This, however, is a merely formal position, given that the powers of Head of Government are assigned to Australia's Governor General, who exercises the monarch's powers in their absence.[193] Legislative power in Australia is exercised by the Federal Parliament,[194] which is comprised of two chambers. The Senate, or the upper house, is composed of representatives divided equally between all the states of the Commonwealth, and the House of Representatives, or lower house, elected directly by the citizens. Judicial power is exercised by the High Court, Australia's highest court; underneath it are found the Federal Court of Australia, a family court, and finally the Federal Magistrate's Court of Australia, established in 1999.[195] Australian politics features two principal parties, the Liberal Party and the Labor Party[196]; in 2007, the latter, under the leadership of Kevin Rudd, defeated the John Howard's Liberal government. If the principal question during the Labor electoral campaign was Australia's participation in the Iraq conflict, a fundamental role was also played a number of issues related to the *digital world*, including, for example, the promise to increase access to broadband connections throughout the country. During his political campaign, Stephen Conroy, the shadow Minister of Employment, Communications and Information Technology, published the proposal of a detailed *cyber-security plan*[197] highlighting the significance of a regulation, aimed to pro-

[193] See http://australia.gov.au/. Accessed 19 November 2011.

[194] See http://www.aph.gov.au/index.htm. Accessed 19 November 2011.

[195] See the Federal Magistrates Court web site: http://www.fmc.gov.au/. Accessed 19 November 2011.

[196] See http://www.alp.org.au/. Accessed 19 November 2011.

[197] The public announcement of the Cyber White Paper by Senator the Hon. Stephen Conroy, Minister for Broadband, Communications and the Digital Economy, Deputy Leader of the Government in the Senate and Minister Assisting the Prime Minister on Digital Productivity, is at the address http://www.minister.dbcde.gov.au/media/media_releases/2011/198. Accessed 20 November 2011. The paper will cover a broad range of areas including consumer protection, cyber safety, cyber crime, cyber security and cyber defence.

tect children from inappropriate or harmful materials, that obliged ISPs to filter contents from a black list issued by the *Australian Communications and Media Authority* (ACMA).[198] Once the elections were over, the Labor Party vowed to maintain their campaign promises and to implement plans for child online safety programs. In fact, Rudd's first budget featured over 128 million dollars for cyber security. However, since that time, the government's attention appears to have shifted from the question of restrictions on inappropriate materials for *children* toward blocks and filtering of *all* content considered generally undesirable. Thus the Australian government has now initiated a filtering program, rendering illegal or inappropriate online content completely inaccessible. This new censorship campaign has lead to indignant protests and online petitions throughout the country,[199] and has received the nearly universal condemnation of the Australian press.

As Bambauer commented (Bambauer 2008), Australia's decision to implement Internet censorship using technological means creates a natural experiment: the first Western democracy to mandate filtering legislatively, and to retrofit it to a decentralized network architecture (Bambauer 2008: 1), putting the country at the forefront of the spread of this practice from authoritarian regimes such as China and Iran to

[198] See the ACMA web site at the address http://www.acma.gov.au/WEB/HOMEPAGE/PC=HOME. Accessed 19 November 2011.

[199] See, *inter alia*, the *United Nations Youth Association of Australia* "Internet Censorship Blue Paper" of December 2008 (http://unyouth.org.au/assets/Documents/bluepapers/Blue-Paper-Censorship.pdf. Accessed 13 November 2010). The authors of this document " […] strongly support the Government in its efforts to prevent access to, especially by young people, illegal material such as child pornography [but] are, however, concerned by the lack of clarity around what constitutes the "harmful and inappropriate" material the Government is also seeking to ban access to with its mandatory ISP-level filtering" (UNYA 2008: 1) and believe that better Internet education offers the best possible opportunities to limit the potential harm of dangerous online material (UNYA 2008: 2). The two main points discussed in this document regarding the filtering systems are: 1. The Government must explain why a 'harmful and inappropriate material' category is necessary and provide an unambiguous definition of 'harmful and inappropriate', and 2. ACMA's blacklisting process must be subject to a transparent review and appeals system (UNYA 2008: 4). The three topical aspects of ISPs actions are: 1. It would only ever be appropriate to introduce ISP-level filtering when the technology causes no or only negligible network degradation. 2. ISP-level filtering should be used to enforce bans on blacklisted (i.e. illegal or prohibited) material but users should be empowered to decide for themselves what is harmful and inappropriate. This means either self-filtering or opting-in to the Government's clean-feed. 3. Emphasis needs to be shifted onto better cyber-safety and general cyber education for both young people and parents (UNYA 2008: 8). Conclusions of the report are that: 1. The Government should provide full and frank reporting of its completed and any future live pilots. The Government should also disclose the objectives outlined for the pilot and the circumstances in which the pilot is being completed. 2. The Government must clarify the future of its plans for internet censorship to allow for greater public debate of the issues surrounding its policy. 3. Internet censorship can threaten human rights, rights Australia is obligated to guarantee under international law. Education to ensure that Australians can make responsible and informed choices is a better approach to reducing potential harm than censorship (UNYA 2008: 9–10).

Western democratic nations and create a fascinating natural experiment in Internet censorship by Western democracies (Bambauer 2008: 2).

6.2.11.2 The Australian Legal System

Australia's judicial system is based on the Constitution of the Commonwealth of Australia[200]; approved in 1900, it may be modified only by referendum. This fundamental body of law, however, contains no explicit laws guaranteeing the freedoms of speech or of expression (although the High Court has ruled that an implicit right to these freedoms does exist). Restrictions and protections of this right therefore derive principally from the democratic political process. The lack, however, of a law expressly establishing the existence, scope and applicable limits to the freedom of expression allows the Australian government a much larger range in which to maneuver with regard to online censorship as compared to other countries, such as the United States, in which the First Amendment to the Constitution specifically protects the freedom of expression. Thus the government of Australia was able to implement censorship activities legally, when legislation concerning internet censorship, the *Broadcasting Services Amendment* (*Online Services Law*), went into effect on January 1, 2000.[201] This law originated as a bill presented to Parliament by the Liberal party; the Liberal bill, however, was substantially changed during the ratification process. In fact, had that bill had been approved without such modifications, today Australian ISPs would be obliged to block all adult access to *any* "inappropriate" or illegal online content or risk to substantial fines and other sanctions, even for content hosted outside the country. However, upon wide condemnation of the restrictive nature of the bill, it was revised to take on its present form, and was subsequently ratified by Parliament.

The Internet censorship established by the BSEB in 1999 is a complaints-based system, and thus content to be blocked is generally identified on the basis of complaints made to the *Australian Communications and Media Authority* (AMCA) (until July 2005 known as the *Australian Broadcasting Authority*), which has the power to examine all complaints filed regarding content that is, or appears to be, offensive or illegal. The AMCA is not obliged to search the Internet for prohibited content, although it does have the right to independently initiate investigations without having received a specific complaint. The ACMA has developed an online complaint system, in order to render making complaints easier for Australian citizens.

Content of published materials is prohibited generally only after a complaint has been lodged, an investigation has taken place and the content in question has effectively received one of the following ACMA classifications: R18, contains material that may be disturbing or harmful to those under 18; this type of content may

[200] Available at http://www.aph.gov.au/senate/general/constitution/. Accessed 20 November 2011.

[201] Available at http://www.comlaw.gov.au/Details/C2004B00465. Accessed 20 November 2011.

additionally be completely prohibited on domestic hosting sites lacking age-verification systems certified by the ACMA. The law applies only to Australian ISPs, and therefore does not affect R18 content on sites hosted on foreign servers; X18 (nonviolent sexually explicit content between consenting adults); RC (Refused Classification, prohibited on Australian-hosted websites). The law also addresses content that is "potentially prohibited", defining in Section 1 such materials as that content not yet classified by the Classification Board, but that, in all probability, would be classified as such it were to be examined. This classification system was established by the Classification (Publications, Film and Computer Games) Act of 1995[202] and is part of a classification scheme adopted by the Commonwealth for films, publications and computer games. It is important to note that the law differs based on the media considered, and is thus much less restrictive, for example, with regard to printed materials as compared to films or videogames. The development and wide scale availability of Internet throughout Australian territory occurred some years after the creation of this law and the Commonwealth's classification scheme, and therefore the law was not in fact created with this type of media in mind. Only later did lawmakers decide that, given that the internet displays text but also images and video, it should be subject to the entire body of laws and legislation regulating films, which, as mentioned above, is far more restrictive than the regulations relative to printed materials and newspaper articles. However, this created a situation of enormous disparity, that has yet to be redressed, given that in the event the same material were published both in print and on the Internet, the online version and the print version would be subject to substantially different classification criteria, clearing the way for situations in which the same publication might be considered accessible based solely on whether it is published in print form or online.

Once content has been classified, the ACMA issues a take-down notice formally advising that the material in question must be eliminated.

However, prohibited content is treated differently based on whether or not it is hosted on servers subject to Australian legal jurisdiction. In fact, when content has been found to be offensive and is hosted in Australia, the AMA sends the take-down notice to the ISP hosting it, advising that the material must be eliminated. But if the content is hosted on a site outside Australian jurisdiction, the AMCA proceeds with the technological filtering of the illicit content.

6.2.11.3 Surveillance Techniques, Filtering Systems and Circumvention Tests

In order to enforce the laws and regulations outlined above, the Australian government has instituted a filtering system that blocks material specified on a secret blacklist drawn up by the ACMA, and not open to consultation by Australian citizens. Current government plans, however, appear to involve the creation of a two-tier content

[202] Available at http://www.austlii.edu.au/au/legis/cth/consol_act/cfacga1995489/. Accessed 20 November 2011.

filtering system. The first level would completely block access to Internet content that is for any reason deemed illegal by Australian law and would be mandatory for everyone. The second level would be more limited and would filter only material classified as being inappropriate for children, such as pornography and violence, and would include an opt-out option for users, allowing them to bypass the filters if they desire to do so. This type of filter has been tested for some time in several Australian states, and it has become quite apparent that content filtering poses a number of problematic issues. First of all, the testing period has revealed the government's complete ambiguity regarding the definition of illegal and restricted content. In fact, given that the ACMA blacklist is kept secret,[203] it is not possible to verify the effective illegality of blocked content. Secondly, it must be noted that the government's proposed filtering plan, when it is implemented, will in all likelihood have as its first consequence a significant slowing of the web in Australia, which is already quite slow. This issue is creating numerous problems, not only technical but at the political level as well, given that on the one hand the government keenly desires to exert more control over the Internet, but at the same time, as mentioned above, one of the key promises of the current government has always been that of augmenting broad band availability and web speed.

Due in part to these issues and to the numerous protests by groups supporting digital liberties, the use of filtering products is currently still voluntary (opt in). Australian ISPs are not legally obliged to install filtering software or to block access to any site, and web users are not legally obliged to utilize filtering software or to purchase the filtering products that are offered or made available by the country's ISPs. With regard to precisely this issue, the ACMA issued a sector behavior code in order to induce Australian ISPs to make filtering software products available to their clients, who, however, are not required to utilize them. ISPs choosing to do so may select from a variety of different Internet filtering software, which however presents a problem of a yet different sort. In effect, if ISPs utilize filtering software created by private industry, the choice of exactly what constitutes offensive material is transferred from the Australian government to the private developers of the software products utilized, resulting in a potentially serious transfer of the regulatory process away from the government and even further from the citizens it represents. As we have seen, in fact, with relation to content classification, Australia has a fairly well defined regulatory and legal framework. Nonetheless, these laws might not be respected by software developers, who, unlike government are in no way subject to the judgment of the electorate and therefore are never called upon to answer directly

[203] On 18 March 2009 WikiLeaks published a document, "Australian government secret ACMA internet censorship blacklist", with a list containing 2,395 webpages or site variations derived from those secretly banned by the Australian Communications and Media Authority (ACMA) and used by a government approved censorship software maker in its "ACMA only" censorship mode. In December 2008, WikiLeaks released the secret Internet censorship list for Thailand, remarking that of the sites censored in 2008, 1,203 sites were classified as "lese majeste", criticizing the Royal family. Similar to Australia, the Thai censorship system was originally presented as a mechanism to prevent the child pornography.

to the country's citizens for the choices they make. This transfer of responsibility might in fact be something of a comfortable choice for the government's decision-makers, in that it allows leaders to sidestep any criticism resulting from blocked content, in that they are effectively not responsible for such choices in the eyes of the citizens.

At present, and as we have seen, there is very little transparency surrounding Australia's proposed Internet filtering system. The government has remained quite vague about the material it intends to block and about the ways in which it intends to go about it. This uncertainly makes it very difficult for the country's citizens to assess whether the concrete application of the law is appropriate, and whether the actions proposed are truly the best way in which to accomplish the goals and motivations on which the censorship legislation was originally based. The Labor government has been unforthcoming as to the sites it intends to block and the specific methods to be used. Therefore, a number of transparency measures are desperately needed in order to permit the government to communicate clearly with regard to the targets and modalities of the proposed filtering system. Only then will it be possible for Australia's citizens to adequately assess the initiative.[204]

As Bambauer observes (Bambauer 2008), the concern is that, as filtering is increasingly adopted in Western democracies, censorship that blocks access to material rather than legal measures that punish access after the fact will become increasingly seen as normal rather than problematic. But filtering carries considerable costs in overblocking, transparency, and accountability that may not be evident initially, and censorship can be an effective tool, but it is a dangerous one (Bambauer 2008: 31).

In 2008, a team of scholarsfollowing the announcement of the of a national -level internet filter trial in Australia, decided to test and compare three of the most popular free tools that allow the circumvention of internet censorship devices, such as those used in China. Tests were conducted using three software packages, Freegate, GPass and GTunnel, which were analysed through packet capture to determine their likely effectiveness against the methods it was believed would be employed by the Australian trials. The tests clearly indicated that all three applications provide an easy means of subverting any likely filtering method, with GPass and GTunnel the more suitable candidates, given that Freegate still allowed for plain-text DNS requests (Smart et al. 2008). The first step of the investigation was to select three of the most popular freely available programs that allowed for the bypassing internet content filters: GTunnel, FreeGate and GPass, each of which functions in a slightly different manner, using different infrastructure or methods of bypassing internet

[204] See the essay written by a young Australian scholar (Travaglione 2009) remarking that " […] the government's decision to impose legislative filters on internet content constitutes an unnecessary, illegitimate and irrational attempt by the Government to control information flow in the private sphere. Regulation of the internet is both technically impossible and morally reprehensible, creating a greater scope for internal government corruption. Alternatives such as voluntary internet filters offer consumers true choice as well as offering a superior means of protecting children from potential harm over the internet; allowing parents to truly regulate the content to which their children are exposed without unnecessary government intervention" (Travaglione 2009: 11).

content filters (Smart et al. 2008: 1–2). The second step of the test was to evaluate each of the tools' usage in terms of bypassing internet content filtering and to understand, first, how each of these content filtering methods functions. The scholars highlight three main types of internet content filtering: (i) DNS request filtering, (ii) web page content filtering and (iii) IP address filtering, and in each of these cases there is a different method of bypassing these restrictions (Smart et al. 200 8: 5). The team's conclusions were clear: both GPass and GTunnel support all the defined methods for bypassing internet content filters (Route DNS requests though an encrypted tunnel, Route web traffic through an encrypted tunnel and Route all traffic through an encrypted tunnel); however, FreeGate sends all DNS requests openly through the internet and as such it would be possible for a third party to determine the domain names on which content may have been retrieved, but not the details of which content was retrieved, as that information is encrypted. It would also be possible for a content filtering system to intercept and block DNS requests for domains which are considered to be objectionable or otherwise undesirable by the governing body controlling the filtering system. It can thus be seen that both GPass and GTunnel would allow for content filtering to be bypassed entirely, while FreeGate does not meet the DNS tunnelling requirement and as such may be unsuitable for accessing prohibited content when behind an internet content filtering system (Smart et al. 2008: 5). Anyone with a rudimentary knowledge of search engines would be able to locate free software to bypass such censorship, and three of the most popular free tools for ensuring internet privacy and bypassing censorship firewalls would likely function well against the likely measures to be implemented at the ISP level.

6.2.12 Iceland: Digital Resistance Issues and Freedom of Information

6.2.12.1 Institutions, Legal Framework and Connectivity

It seems also appropriate, in this chapter, to deal with the legislative and political situation of a country, Iceland, which is not indicated, in this book, as a symbol of repression or violations of the freedom and of the fundamental rights, but, on the contrary, as a symbol of modernity in the approach to issues related to the Internet and to the freedom of information.

Iceland is a parliamentary republic, and the oldest democracy in the world. The country's Parliament, called the Althing[205] was founded in 930 AD,[206] during Iceland's Commonwealth period, although its current formation dates back to

[205] See the official web site of the Parliament at the address http://www.althingi.is/vefur/upplens.html. Accessed 19 November 2011.

[206] See the constitutional history of the Parliament at the address http://www.althingi.is/pdf/Althingi2010_english.pdf. Accessed 19 November 2011.

1845. While it is not a member of the European Union, it is part of the European Economic Area (EEA) and has agreed to adopt a legislation that is in force in the countries forming the European Union, especially relating to issues such as consumer protection and commercial law. The principal role of Iceland's Parliament is to balance the executive branch, that is to say, the government,[207] with the needs and duties of the public administration as a whole. The two parliamentary bodies that are most important in this sense are the National Audit Bureau and the Ombudsman. In accordance with the Icelandic Constitution,[208] the Althing and the President of the Republic[209] hold legislative powers jointly. The President is elected by direct popular vote and serves a 4-year term. The Government has an important role in the legislative process, preparing the texts of the countries laws, which are then ratified by Parliament, and exercising wide powers with respect to the content of laws and regulations. The Icelandic judicial system consists of the Supreme Court,[210] responsible for interpreting the country's laws, and of a number of district courts, whose principal source is the Constitution of the Republic, approved in 1994 and modified several times, most recently in 1999.[211] The country's legal system[212] is regulated by two procedural codes (civil and criminal[213]), and, most relevant to the subject of the present analysis, a *privacy law*[214] and a law addressing *the freedom of information.*[215]

Iceland established its first Internet connection in 1986, when the Institute of Marine Research in Iceland was linked to the EUnegt (European Unix Network) in Amsterdam using a UUCP (Unix-to-Unix-Copy) line. The first available connections afforded only electronic mail and Usenet access with a bandwidth of 300 and 1200 bits per second (bps). Today, however, according to data gathered by the Organization for Economic Cooperation and Development (2009), in Iceland 83.2% of all families have access to wideband Internet connections and 99.5% of all businesses use the Internet for their commercial activities.

[207] See the official Government's web site at the address http://www.government.is/. Accessed 19 November 2011.

[208] See the text of the Constitution of the Republic of Iceland at http://www.government.is/constitution/. Accessed 19 November 2011.

[209] See the web site of the President of Iceland at http://www.forseti.is/. Accessed 19 November 2011. The English language version is at the address http://english.forseti.is/. Accessed 19 November 2011.

[210] See the web site of the Supreme Court at http://www.haestirettur.is/. Accessed 19 November 2011.

[211] See the Law n. 33, 17 June 1944, as amended 30 May 1984, 31 May 1991, 28 June 1995 and 24 June 1999.

[212] See at http://www.althingi.is/lagas/nuna/kaflar/kaflar.html. Accessed 19 November 2011.

[213] See at http://www.althingi.is/lagas/139a/1940019.html. Accessed 19 November 2011.

[214] See at http://www.althingi.is/lagas/139a/2000077.html. Accessed 19 November 2011.

[215] See at http://www.althingi.is/lagas/nuna/1996050.html. Accessed 19 November 2011.

6.2.12.2 Protection of Individual Privacy and the Freedom of Speech

The Icelandic Constitution contains two articles directly addressing the rights to *freedom of expression* and to the *freedom of speech*, namely Articles 71[216] and 73.[217] In particular, Article 71 establishes the right to privacy of every individual, in general, with respect to his or her private sphere, and, in particular, with respect to all personal data communicated in any fashion. This right may be limited only by legal authorities or in order to protect the rights of another individual. Article 73 addresses freedom of expression, and establishes that this right may not be legally censured for any reason whatsoever. The only limitations, continues the same article, are those that might be necessary for reasons of public interest, to safeguard state security, or the health and well-being of others, and may only be implemented by a judicial decision or statutory provision.

As mentioned above, Iceland's legislation also includes a law addressing the freedom of information, Law no. 50 of 24 May 1996, which represents the most important piece of legislation concerning this issue in Iceland. The law went into effect on 1 January 1997, but has been amended several times.[218] Similarly to the Constitution, Law 50/1996 also provides very few possibilities for limitations to the free circulation of information. In particular, two articles, 5 and 6, establish that limitations to the free circulation of information may be enacted only to preserve, respectively, private and public interests, and largely reiterate the principles contained within the Constitution. In fact, Article 5 expressly safeguards the interests of important financial and commercial enterprises, while Article 6 establishes that free access to information may be restricted only when necessitated by vital public interest, and specifically, in the event of threat to at least one of the following: (i) the security or the defense of the nation, (ii) relations with other countries or international organizations, and (iii) state-owned enterprise.

---

[216] The text of Article 71: "Everyone shall enjoy freedom from interference with privacy, home, and family life. Bodily or personal search or a search of a person's premises or possessions may only be conducted in accordance with a judicial decision or a statutory law provision. This shall also apply to the examination of documents and mail, communications by telephone and other means, and to any other comparable interference with a person's right to privacy. Notwithstanding the provisions of the first paragraph above, freedom from interference with privacy, home and family life may be otherwise limited by statutory provisions if this is urgently necessary for the protection of the rights of others."

[217] The text of Article 73: "Everyone has the right to freedom of opinion and belief. Everyone shall be free to express his thoughts, but shall also be liable to answer for them in court. The law may never provide for censorship or other similar limitations to freedom of expression. Freedom of expression may only be restricted by law in the interests of public order or the security of the State, for the protection of health or morals, or for the protection of the rights or reputation of others, if such restrictions are deemed necessary and in agreement with democratic traditions."

[218] Amended by Act 76/1997 (entered into force on 1 July 1997), L. 83/2000 (entered into force on June 2, 2000, except Article 1. which took effect on 1 January 2001), L. 23/2006 (entered into force on May 3, 2006; EEA Agreement: XX. Annex Directive 2003/4/EC), L. 161/2006 (entered into force on 1 January 2007), L. 88/2008 (entered into force on 1 January 2009 unless interim provisions. VII, which took effect on 21 June 2008) and L. 55/2009 (entered into force on 1 May 2009).

In relation to the protection of individual privacy, Article 4 of Law no. 77 of 23 May 2000 establishes that electronic surveillance is subordinated to the principle of the *true necessity* of the use of such instruments, and that their implementation must conform to all provisions set forth by that law. Additionally, Article 5 establishes certain exceptions to the protection of privacy (of personal information) in the interest of journalism, art, or literature, on condition that all relative data be utilized only for such purposes.

6.2.12.3 The *Icelandic Modern Media Initiative* Reinforcing the Freedom of Information and the Protection of Journalism

As a result of the country's economic crisis in 2008, Iceland changed its approach regarding the freedom of information and of the press. The cause of the crisis was found to be due above all to the *absence of transparency* in the communication of information by the media and to the suppression of the true dimensions of the situation. The Icelandic parliament realized that the right of its population to know and understand the events occurring in their country needed to be significantly reinforced, and to do this it was clear that it would be necessary to support the free circulation of information and journalism and news reporting activities with improved legislation.

Thus, on 16 June 2010, the Althingi unanimously improved a proposal for a parliamentary resolution requesting the government to introduce a new legislative regime aimed at protecting and reinforcing the freedom of information, with particular attention to investigative journalism and the participation of citizens in the information process. The parliamentary resolution gave rise to a national initiative of broad scope, which is currently supported by a number of European countries, and now known as the *Icelandic Modern Media Initiative* (IMMI).[219]

The proposed legislation package would include an extensive reform to the current legal framework, especially in relation to the protection of journalistic sources, currently established by Article 119 of Law no. 88/208, which provides for the right of journalists to refuse to reveal their sources, unless they are requested to do so by a court of law. This provision will be modified, because the exceptions to the protection of sources are considered too broad and additionally in contrast with the European Union Council Recommendation n. R (2000)7, which additionally is also contrasted by the *Right to Information Law* currently in force (Law 50/1996). The latter, moreover, does not conform to the standards established by the Aarhus Convention on Access to Information in Environmental Matters.[220]

---

[219] See the text at http://immi.is/Icelandic_Modern_Media_Initiative. Accessed 19 November 2011.

[220] See the text at http://europa.eu/legislation_summaries/environment/general_provisions/l28056_it.htm. Accessed 19 November 2011.

With the IMMI, Iceland has the opportunity to create a legal framework of international scope to protect maximum transparency in the free circulation of information.

The proposal voted upon and approved by Parliament was not the final legislation, but rather began the creation of a legislative *corpus* involving the modification of at least 13 existing laws based on the specifications of the proposal. The process should reach completion by mid-2012. Among the issues to be further elaborated are, as mentioned above, the freedom of information and the freedom of the press, with the aim of guaranteeing and encouraging the highest levels of popular participation in the decisions taken by the government.

At the base of the IMMI are, also, the provisions included in the directives and indications of the European Council on Freedom of the Press issued in 2009. Additionally, the IMM seeks to reproduce a number of provisions already in force in numerous countries around the world. For example, it is partially modeled after the *Federal False Claims Act* (31 USC paragraphs 3729–3733) of the United States of America, which protects and provides incentives for those who reveal cases of fraud against the government.

The IMMI is obviously supported by organizations such as *WikiLeaks* and *Global Voices*, seeking to augment transparency by publishing information that may be "uncomfortable" for multinational corporations or governments. For these organizations, the future legal framework of Iceland, with its new regulations and laws, will be an invaluable resource that will allow them to operate freely and unhindered by the threat of legal action against them.

However, there are those who fear that the principles behind the IMMI could spread to other jurisdictions. The rigid libel laws and strict courts in certain countries have led to a phenomenon known as "lawsuit tourism". In essence, lawsuits, often involving libel or defamation, are filed against journalists in those countries in which it is most probable to win the case; however, with a legal framework based upon the principles of the IMMI, this would no longer be possible.

In recent years, the freedom of information and of the press has been repeatedly stifled in a number of countries throughout the world, including both those headed by authoritarian regimes, but also in a number of countries that are not generally deemed particularly repressive at all.

Thus with the IMMI Iceland might become far more than simply a safe haven for the freedom of the press or a paradise for international investigative journalism, but a model and inspiration of legal systems everywhere.

6.2.13 India: Freedom of Speech, Freedom of Information and Electronic Censorship

6.2.13.1 Internet and ICT in India: A Brief Overview

India, with a population of 1.2 billion, is the world's second most populous nation, and it's seventh largest in terms of geographical extension. While Internet penetration rates,

in 2010 estimated at approximately 7%, are quite low as compared to global standards, cellular telephone use, thanks in part to the introduction of a number of new, more economic telephone plans, is growing considerably, with a user rate that was recently estimated to be equal to approximately 60% of the country's population.[221] Overall, there are 81 million Internet users in India and, according to estimates, this number should triple by 2015.

The availability of information and communication technologies has increased significantly following the liberalization of the country's telecommunications sector beginning with the *New Economic Policy*, approved in July 1991. The sector is regulated by the *Telecom Regulatory Authority of India* (TRAI), an independent body created by Parliament in 1997 with authority over ISPs and mobile telephones.[222] In the context of the Indian economy, the IT sector plays a decisive role, with a turnover of 88 billion dollars and 2.5 million qualified workers.[223]

Despite this rapid expansion, however, significant obstacles to Internet access remain; limited infrastructure, high connection costs and low literacy levels are some of the serious problems that have yet to be resolved, especially in rural regions, in which vast areas are still without electricity. The urban–rural divide, while diminishing, is still quite marked, with only 4.18 million active users out of an overall rural population of approximately 800 million inhabitants. Wide band access, despite the Indian government's having included plans for its growth since 2004, is still quite limited. However, significant recent public and private investments aim to guarantee both considerable increases in wide band availability and a reduction in connection costs by 2012.[224]

6.2.13.2 Freedom of Speech and the Legal Framework

The freedom of speech, at least formally, is fully protected under Indian legal and regulatory frameworks. India's Constitution, ratified in 1959, is its primary source of statutory law. Article 19, entitled *Rights to Freedom*, guarantees a number of fundamental rights, among them the freedom of speech and the freedom of expression, while at the same time reserving the authority of the state to impose restrictions

[221] See the data published on the web site of the The Boston Consulting Group (Report 2010). Digital Consumers in Brazil, Russia, India, China and Indonesia. http://www.bcg.com/documents/file58645.pdf. Accessed 16 October 2011.

[222] See the official web site at http://www.trai.gov.in. Accessed 16 October 2011.

[223] See Department of Information Technology and National Policy of Information Technology. http://india.gov.in/allimpfrms/alldocs/16391.pdf. Accessed 16 October 2011.

[224] See Freedom House (2011). Freedom on the Net 2011. India. http://www.freedomhouse.org/images/File/FotN/India2011.pdf. Accessed 16 October 2011.

to those rights, in the interests of the sovereignty and integrity of India, state security, foreign relations, public order, decency, or morality, or in relation to defamation or incitement to an offence.[225]

The country's ITC sector is governed by a vast complex of laws and regulations, including articles from the code of criminal procedure and the criminal code, the *Indian Telegraph Act* of 1885 and its subsequent modifications and amendments, and the *Information Technology Act* of 2000 (no. 21/2000). Following the 2008 terrorist attacks in Mumbai, the government has consolidated its power of surveillance over the country's communications. In this context, the government issued the 2008 *Information Technology Act*, which went into effect on 27 October 2009, introducing new and stringent electronic censorship and content monitoring measures.[226] In particular, the changes to Article 69 extended the circumstances in which the government is authorized to *intercept*, *monitor* and *decipher* information generated,

[225] See the text of the Constitution of India at the address http://india.gov.in/govt/documents/english/coi_part_full.pdf. Accessed 16 October 2011. The text of Article 19 is: "[…] (1) All citizens shall have the right (a) to freedom of speech and expression; (b) to assemble peaceably and without arms; (c) to form associations or unions; (d) to move freely throughout the territory of India; (e) to reside and settle in any part of the territory of India; and […] (g) to practise any profession, or to carry on any occupation, trade or business. (2) Nothing in sub-clause (a) of clause (1) shall affect the operation of any existing law, or prevent the State from making any law, in so far as such law imposes reasonable restrictions on the exercise of the right conferred by the said sub-clause in the interests of the sovereignty and integrity of India, the security of the State, friendly relations with foreign States, public order, decency or morality, or in relation to contempt of court, defamation or incitement to an offence. (3) Nothing in sub-clause (b) of the said clause shall affect the operation of any existing law in so far as it imposes, or prevent the State from making any law imposing, in the interests of the sovereignty and integrity of India or public order, reasonable restrictions on the exercise of the right conferred by the said sub-clause. (4) Nothing in sub-clause (c) of the said clause shall affect the operation of any existing law in so far as it imposes, or prevent the State from making any law imposing, in the interests of the sovereignty and integrity of India or public order or morality, reasonable restrictions on the exercise of the right conferred by the said sub-clause. (5) Nothing in sub-clauses (d) and (e) of the said clause shall affect the operation of any existing law in so far as it imposes, or prevent the State from making any law imposing, reasonable restrictions on the exercise of any of the rights conferred by the said sub-clauses either in the interests of the general public or for the protection of the interests of any Scheduled Tribe. (6) Nothing in sub-clause (g) of the said clause shall affect the operation of any existing law in so far as it imposes, or prevent the State from making any law imposing, in the interests of the general public, reasonable restrictions on the exercise of the right conferred by the said sub-clause, and, in particular, nothing in the said sub-clause shall affect the operation of any existing law in so far as it relates to, or prevent the State from making any law relating to,— (i) the professional or technical qualifications necessary for practising any profession or carrying on any occupation, trade or business, or (ii) the carrying on by the State, or by a corporation owned or controlled by the State, of any trade, business, industry or service, whether to the exclusion, complete or partial, of citizens or otherwise".

[226] See The Information Technology (Amendment) Act 2008 at http://www.mit.gov.in/sites/upload_files/dit/files/downloads/itact2000/it_amendment_act2008.pdf. Accessed 16 October 2011.

transmitted, received or conserved in any computer resource.[227] Secondly, the amendment augmented the number of criminal acts (in the introduction to Articles 66A-B-C-D-E of the ITA, 2000), which thus now also include sending offending messages, identity theft, violation of privacy, cyber terrorism and the publication and transmission of content that is obscene or in any way related to child pornography.[228] The amendment also created strict obligations for *intermediaries*, with prison sentences of up to 7 years for the representatives of a vast array of private services, including providers, search engines and cybercafés, who do not conform to the government's content filtering program. Moreover, the amendment also contained a number of provisions directed specifically toward Internet cafés which, in addition to for the first time being legally defined, were also expressly included among intermediaries, and thus subject to a series of strict obligations reserved for Internet intermediaries.[229] *Guidelines for CyberCafès* establishes that Internet café owners must register with an especially-created agency, identify all clients, maintain a register of all users for at least 1 year, keep and send to the government a monthly visitor log and clearly post signs prohibiting access to content that is pornographic or otherwise against the law.[230] Finally, cybercafé owners are also required to submit a detailed monthly register indicating all online activity for all computer resources. In addition to the rigid legal provisions, reports of police intimidation of cybercafés are frequent.

6.2.13.3 Digital Censorship, Filtering Tools and Repression in India

The Indian government has not enacted any wide-scale policies or strategies to block access to ICT. Currently, there are no restrictions regarding access to web applications such as *YouTub*e, *Facebook* or *Twitter*, which, together with *Orkut*, are among the most popular web sites in the country. Moreover, the country has an extremely active blogosphere, which, although it is divided between the many available

[227] The text of Article 34 of The Information Technology (Amendment) Act 2008 is: "Art. 34 (Section 69 A 1): Where the Central Government or any its officers specially authorized by it in this behalf is satisfied that it is necessary or expedient so to do, in the interest of sovereignty and integrity of India, defence of India, security of the State, friendly relations with foreign State or public order or for preventing incitement to the commission of any cognizable offence relating to above, it may subject to the previsions of sub – section (2), for reasons to be recorded in writing, by order, direct any agency of the government or intermediary to block for access by the public or cause to be blocked for access by the public any information generated, transmitted, received, stored or hosted in any computer resource".

[228] See The Information Technology (Amendment) Act 2008. Art. 34.

[229] See The Information Technology (Amendment) Act 2008. Art. 4, letters D and H.

[230] See GSR 315(E) Dated 11 April 2011: Information Technology (Guidelines for Cyber Cafe) Rules, 2011 at http://www.mit.gov.in/sites/upload_files/dit/files/GSR315E_10511(1).pdf. Accessed 16 October 2011.

blogging platforms, is relatively free to express itself as it wishes. However, certain topics must be addressed with extreme caution in India and, especially in recent years, there has been a noticeable increase in both measures seeking to remove content perceived as obscene or representing a danger to public order or national security and legal action against users for opinions expressed online. Government initiatives, up to the present, apart from a uniform strategy, have been often inconsistent and at least partially ineffective.[231]

India's Internet filtering regime is implemented by the *Computer Emergency Response Team* (CERT-IN), an agency forming part of the *Ministry of Communication and Information Technology* (MCIT) and empowered to protect national security in cyberspace and to prevent and manage computer security incidents.[232] In order to complete its mission ("to enhance the security of India's Communications and Information Infrastructure through proactive action and effective collaboration") the CERT-IN reviews complaints and issues blocking instructions for specific web sites deriving from a pool of government-specified officials. After having verified the authenticity of the complaints and the effective necessity of blocking the site, the agency provides instructions to the *Department of Telecommunications.*[233] The order is then sent to all the country's ISPs, all of which must obligatorily conform to the decision. With very few exception, the blocking mechanism created under the Act provides for no review or appeal procedures, except in court, and is permanent in nature. Additionally, when CERT-IN has issued orders to block specific web sites, no communication has been made to the public beforehand.[234]

Content filtering is also implemented through certain specific clauses, included in the licenses issued to ISPs, mandating the surveillance of all traffic, the blocking of users or Internet sites as specified by the TRAI, and the adoption of filtering devices for obscene materials.[235]

Surveillance tools are also provided to telecommunications companies, who are regularly "invited" to reveal their security codes or to consent to other methods allowing authorities to intercept client traffic. Based on the guidelines issued in 2010 conferring wide powers upon authorities in order to combat terrorism and protect national security, such requests have also included *BlackBerry* services, as well as its instant messaging service. The Indian government threatened to shut down those services if RIM (*Research in Motion*) did not permit the surveillance of traffic on its devices by 30 August 2010.

---

[231] See the ONI *Country Profile* regarding India at http://opennet.net/research/profiles/india. Accessed 16 October 2011.

[232] See http://www.cert-in.org.in/. Accessed 16 October 2011.

[233] See Notification no. GSR. 181(E), dated February 27, 2003 at http://www.mit.gov.in/content/it-act-notification-no-181. Accessed 16 October 2011.

[234] See the cited ONI *Country Profile* regarding India.

[235] See the Report by Freedom House (2011). Freedom on the Net 2011.

Recent tests performed by the *OpenNet Initiative* documented multiple episodes of censorship and filtering, generalized surveillance of contents, in addition to frequent surveillance of conversations.[236] In this context, a *Google Report*, made public in 2010, takes on even more significance. The report documented no fewer than 142 government requests for site removal, for the most part carried out by *Google*, during the period extending from 1 July to 31 December 2009.[237] Court proceedings, and guilty verdicts, are fairly frequent against individuals expressing their opinions online. One such episode that generated significant media coverage was the 2007 arrest and detention of Lakshmana Kailash K., following the collaboration with police of both *Google* and one of India's principal ISPs, for having posted insulting images of a revered historical figure on the Internet (it later transpired that the arrest warrant was issued on the basis of a mistaken IP address). Similarly, arrest warrants were issued in 2008 for two Indian citizens for having posted denigratory comments about the President of the Indian National Congress on an *Orkut* community called "I hate Sonia Gandhi". In fact, over the last 2 years *Orkut*, a social networking site, has been blocked on diverse occasions, for political and social reasons.[238]

6.2.13.4 The Freedom of Information and Open Government Data

The *Right to Information Act* was approved by the Indian Parliament in May 2005 and was signed into law by the President the following June.[239] The law guarantees citizens the right to access information not only from Central Government authorities, but also from local authorities and from government-financed bodies and non-governmental organizations, and requires public institutions to publish and distribute a vast array of information.[240] This represents a first important step towards the construction of a dialog between citizens and the public sector, and constitutes a milestone in the transition from a culture of *secrecy* to one of partial *transparency*.

The desire for more openness, at least in the intentions of India's lawmakers, is clear from the definition of accessible information: *"information" means any material in any form, including records, documents, memos, e-mails, opinions, advices, press releases, circulars, orders, logbooks, contracts, reports, papers, samples, models, data material held in any electronic form and information relating to any private body which can be accessed by a public authority under any other law for the time being in force* (Article 2, letter f). But the truly revolutionary content is to

---

[236] See the cited ONI *Country Profile* regarding India.

[237] See the Google Transparency Report at http://www.google.com/transparencyreport/governmentrequests/. Accessed 19 November 2011.

[238] See Freedom House (2011). Freedom on the Net 2011.

[239] See the Right to Information Act, No. 22 of 2005. http://www.fra.org.in/laws/rti.pdf. Accessed 16 October 2011.

[240] See MANISAR, D. (2006). Freedom of information around the world. http://www.freedominfo.org/wp-content/uploads/documents/global_survey2006.pdf

be found just below, in Article 4, paragraph 2, which, taken literally, puts an end to the tradition of the secrecy of information in India, urging authorities to take every effort to proactively publish as much data online as possible, regardless of whether such information has been specifically requested by citizens.[241]

However, the degree of application of this law, after 6 years of its having gone into effect, cannot, unfortunately, be said to be sufficient, and numerous weak points have been reported, including the complete opacity of the procedure of the nomination of Information Commissioners, who are the guarantors of all access procedures and processes (regulated by Articles 12, 13 and 14 of the Law) and the failure to respect both the established time limits and statutory provisions regarding the proactive online publication of information.

While the *open data movement* is slowly picking up speed in India, there are no easily accessible and open public data banks that are re-utilizable (for example, featuring open and machine readable formats), comprehensible (what material there is on Indian official sites, to the contrary, is often only available in *.pdf*, or over a number of different sites or published only aggregate form) and reliable (the absence of clear data collection methodologies leads to significant doubt as to the reliability and accuracy of its sources). As documented by a recent report entitled *Open Government Data in India*, by the *Center for Internet and Society of Bangalore*, there are diverse obstacles to the transparency of government information. One of the most significant is connected to the data collection phase, both because automation of these processes is not yet widely available at all levels of government and because the methods used lack clarity. The situation is further clouded by the lack of understanding, at virtually all levels of society, of the true benefits of open data in the public sector; even when information is available in spreadsheet or other machine readable formats, it is often published as *.pdf* files. Inadequate computer literacy, especially among the more disadvantages levels of the society, is accompanied by the conviction that public data should be safely kept by authorities, so that, among other reasons, it will not end up in the wrong hands.[242] In an effort to further encourage open data in India, in the context of strengthening democracy and supporting the fight against corruption, in 2010, the President of the United States Barack Obama and the Indian Prime Minister Manmohan Singh created a US-India partnership on open government.[243]

---

[241] See the Right to Information Act, No. 22 of 2005. Art. 4, comma 2: "It shall be the constant endeavour of every public authority to provide as much information suo motu to the public at regular intervals through means of communication, including internet so that the public have minimum resort to the use of this Act to obtain information".

[242] Centre for Internet and Society (2011). Report on Open Government Data in India. http://www.cis-india.org/openness/publications/ogd-report (Accessed 16 October). The Indian government portal may be accessed at http://india.gov.in/ (accessed 16 October 2011).

[243] White House. Fact Sheet on United States and India Announce Partnership on Open Government, http://www.whitehouse.gov/sites/default/files/us-india_open_government_partnership.pdf (Accessed 16 October 2011).

6.2.14 Russia. Internet and Human Rights: Political and Technological Frameworks

6.2.14.1 Internet Diffusion in Russia

Extending across two continents, and with a population of nearly 143 million inhabitants, Russia, independent since the end of the USSR and the birth of the *Commonwealth of Independent States* (CIS), is, without a doubt, the area's foremost geopolitical reality. This central importance, united with its considerable natural resources, render Russia, in addition to being a member of the BRIC group of rapidly developing and globally important economies, an interesting object to observe with respect to the topics of digital liberties and democracy in general.

The country created a new Constitution in 1993 but, while this might be apparently significant, that event does not represent a true break with preceding policies; analysts in fact agree that there are significant similarities regarding the conception of power, specifically in its often problematic relationships with individual liberties, regardless of the historical period or the Constitution in force at the time. In this regard, it is important to note that the idea of democracy, and its capacity to adapt to opposing interests, has always been rather difficult for Russians to assimilate, so much so that often the references to democracy made by the country's ruling party (or those of the dominating group in a certain period) have often been atypical, exaggerated and even incongruous.

Despite the proclamations, the amendments and the protests presented at regular intervals by Russian institutions, one conclusion is certain: the Russian conception of *power* has always been, and remain to the present day, autocratic and not democratic, distant from European and occidental legalism. In this perspective, unfortunately, the expression of individual ideas, in any fashion, does not constitute an exception.[244]

The availability of Internet among the Russian population has by now reached levels nearing those of other industrialized countries (28% in 2008, 43% in 2011, with percentages very much in line with those of the industrialized world in large urban centers such as Moscow and Saint Petersburg).[245] The number of individuals using the Internet on a daily basis has grown ten times over the last 8 years and, when *Yandex.ru*, the most famous Russian site, was listed on the *New York Stock Exchange*, the 24 of May 2011, its price rose 55% on the very first day, resulting in gains of

[244] See the United States Department of State, Bureau of Democracy, Human Rights, and Labor (March 2008): "The government does not require Web sites to register as mass media, and unregistered Web sites were not subject to administrative sanctions. Postings on the Internet were subject to the same restrictions that applied to other types of expression, and some bloggers were charged with inciting hatred for their Internet postings". http://www.state.gov/g/drl/rls/hrrpt/2007/100581.htm. Accessed 15 October 2011.

[245] See http://www.internetworldstats.com/stats4.htm. Accessed 13 October 2011.

nearly 1.3 billion dollars. Social media are also in rapid expansion. *Facebook*, *VKontakte*, *Twitter* and *YouTube* are regularly among the most visited Internet sites. The natural indomitability of the web was recently the object of governmental attention, both in terms of its regulation and in strictly technical terms as well.

In terms of this last perspective, and in general, Russia, together with the other CIS countries, has recently transformed its approach with respect to issues surrounding digital liberties. The burdensome obligations, in terms of content control, weighing on website administrators and the dire consequences, in terms of both civil and legal liability, deriving from the publication of *inappropriate* or *defamatory* material, have led to worrisome cases of self-censorship.[246] Moreover, Russia can be considered to be the guiding force behind a number of new web surveillance policies, in particular through the system known as SORM-II. Taking effect in 2000, the protocol allows security forces to physically enter ISP networks in order to check for and, when necessary, to remove illegal materials. It moreover requires burdensome "collaborative" contributions from ISPs, demanding that they (i) register all Internet traffic (including IP addresses, connection times and data transmitted) in order to (ii) provide all such data to the *Federal Security Service* (FSB). This is far from a "measured" system; it is enough to consider those ISPs who saw their licenses revoked for the mere fact of having dared to bring up the potential privacy risks for their clients. Recently a high-level FSB official even requested authorization to intercept *all* Russian mobile telephones with capacities for connecting to the Internet. And this, despite the fact that Russian legislation, at all levels, formally protects personal confidentiality, prohibiting surveillance and recordings of all kinds in the absence of specific legal authorization. In addition to the "structural" interventions mentioned above, aimed at controlling the "daily use" of Internet, also observed throughout the CIS region have been episodes of a new and atypical technique known as "*event-based filtering*", used only in moments of particular political tension, and fairly contained in terms of scope and duration.

In any case, serious doubts remain as to the real possibility of effectively analyzing such large quantities of data.

6.2.14.2 The Legal and Regulatory Framework

The Constitution of the Russian Federation, ratified on 12 December 1993 constitutes the country's primary source of statutory law, and as such is the fitting point of departure for any analysis of the Russian legal system. Specifically, with regard to the freedom of expression, one must look to Paragraph II (Articles 17–64), entitled *Rights and Freedoms of Man and Citizen*. The contents of this section, which expressly grants Russian citizens a number of rights, directly applicable in the country's courts, are substantially equivalent to those forming part of modern European

[246] See http://opennet.net/research/regions/commonwealth-independent-states. Accessed 14 October 2011.

constitutions and international human rights agreements. Specifically, the freedom of information and the freedoms of speech and of expression are guaranteed by Articles 24, paragraph 2 and 29 of the Federal Constitution[247] while Article 23 of the same document guarantees the rights to privacy, data protection and to the secrecy of communications.[248] Finally, Article 55 of the Russian Federal Constitution prohibits any legislation violating or derogating these fundamental rights, except in determined cases, and only as provided by federal law.

Before examining the body of Russian laws pertaining specifically to the communication technology sector, a short preliminary note is in order: Article 24, paragraph 2 of the *Law on Mass Media* provides that the regulations established for radio and television are also applicable to "periodical dissemination of mass information via teletext and videotext system and other telecommunications networks". It is thus evident that all laws applicable to the "classic" press in terms of civil (Articles 150–152 of the *Civil Code*) and criminal wrongdoing are also applicable "online" (see, for example, Articles 129, 140, 141.1, 205.1, 283 and 310 of the *Criminal Code*).[249]

Specific rules, often deriving from Russian case law, regulate the liability of website administrators for posts and offensive content that may be generated by site readers and/or users. In these situations, liability has been found to lie with the website administrator only when, after having been duly informed of the presence of such content, the administrator has neglected to remove the content in question.[250]

The Law on Mass Media, around which a large portion of Russian regulations of this sector rotates, carefully delineates, at least in theory, the sphere of applicability of what is generally defined as the cause of justification of formally illicit conduct. Distributing information on the private lives of citizens is prohibited, unless it is "necessary for the protection of public interests" (Article 50, paragraph 1, subparagraph

[247] The text of Article 24 is: "(1) The collection, storage, utilization and dissemination of information about a person's private life without his consent are not permitted. (2) Organs of State power and organs of local self-government and their officials are obliged to ensure that each person has the opportunity to see documents and materials directly affecting his rights and freedoms unless otherwise provided by law". The text of Article 29 is: "Article 29. (1) Each person is guaranteed freedom of thought and speech. (2) Propaganda or agitation exciting social, racial, national, or religious hatred and enmity is not permitted. Propaganda of social, racial, national, religious, or linguistic supremacy is prohibited. (3) No one may be compelled to express his opinions and convictions or to renounce them. (4) Each person has the right freely to seek, receive, pass on, produce, and disseminate information by any legal method. The list of information constituting a State secret is determined by federal law. (5) The freedom of mass information is guaranteed. Censorship is prohibited".

[248] The text of Article 23 is: "Everyone shall have the right to inviolability of private life, personal and family secrecy, and defence of his or her honour and reputation. 2. Everyone shall have the right to privacy of correspondence, telephone conversation, postal, telegraph, and other communications. Limitation of this right shall be permitted only on the basis of a sudicia decision".

[249] See http://www.lexadin.nl/wlg/legis/nofr/oeur/lxwerus.htm. Accessed 10 October 2011.

[250] See *Supreme Court of the Russian Federation, Resolution* No. 16, 2010, "*On the Judicial Practice Related to the Statute of the Russian Federation 'On the Mass Media'*".

2, Law on Mass Media); divulging and utilizing third-party images in the absence of consent is also prohibited, unless such use is for the express purposes of protecting "*state, social or other public interests*" (Article 152 Civil Code). In relation to this, there are two considerations that must be borne in mind. Firstly, there is clear communicability between the *Law on Mass Media*, which could be defined as causal, and other lateral and consequential norms, such as those contained in the country's civil and criminal codes as well as its privacy laws; these last, in fact, are expressly applicable only in those situations in which the *Law on Mass Media* is not. Secondly, it should be remembered that the ambiguity of concepts such as *public, social* or even *state interest* may have permanent consequences: in addition to rendering the legal precepts themselves uncertain, the resulting risks of rendering perfectly legal conduct punishable by using restrictive interpretations of the above notions are significantly increased. It is perhaps, therefore, in this fundamental task of better and more clearly defining those actions that can and should be sanctioned that the interpretative efforts of the *European Court for the Rights of Man* have been most significant in the Russian context; Article 15, paragraph 4,[251] and Article 17[252] of the Federal Constitution in fact guarantee respect of international treaties ratified by the Duma and of international human rights standards.

Russia's entrance, on 28 February 1996, in the system of the Council of Europe, has additionally lead to the ratification of the Convention on the Protection of Individuals with regard to Automatic Processing of Personal Data on 19 December 2005 which, after several delays and extensions, went info force on 1 January 2011. By virtue of Russia's position on these international agreements, its legislation is perfectly in line with European standards regarding the protection of personal data, placing burdens on the federal and local authorities holding such data. An individual may request a copy of his or her personal data (Article 18) and, generally, the administrator has ten working days in which to fulfill that request. Criminal charges may

[251] See Article 15 of the Russian Constitution: "1. The Constitution of the Russian Federation shall have the supreme juridical force, direct action and shall be used on the whole territory of the Russian Federation. Laws and other legal acts adopted in the Russian Federation shall not contradict the Constitution of the Russian Federation. 2. The bodies of state authority, the bodies of local self-government, officials, private citizens and their associations shall be obliged to observe the Constitution of the Russian Federation and laws. 3. Laws shall be officially published. Unpublished laws shall not be used. Any normative legal acts concerning human rights, freedoms and duties of man and citizen may not be used, if they are not officially published for general knowledge. 4. The universally-recognized norms of international law and international treaties and agreements of the Russian Federation shall be a component part of its legal system. If an international treaty or agreement of the Russian Federation fixes other rules than those envisaged by law, the rules of the international agreement shall be applied".

[252] See Article 17 of the Russian Constitution: "1. In the Russian Federation recognition and guarantees shall be provided for the rights and freedoms of man and citizen according to the universally recognized principles and norms of international law and according to the present Constitution. 2. Fundamental human rights and freedoms are inalienable and shall be enjoyed by everyone since the day of birth. 3. The exercise of the rights and freedoms of man and citizen shall not violate the rights and freedoms of other people".

be filed against those who refuse to provide such data, violate privacy regulations, or illegally access digital data banks. Furthermore, the code of administrative violations establishes punishment for anyone collecting, memorizing, utilizing or distributing personal data in any fashion (13 and 14).[253]

Thus this brief analysis of the Russian legal framework may be concluded with the following observation: despite that fact the Russian Constitution embraces and protects the freedom of speech and the freedom of the press, the various regulatory authorities, through myriad laws, presidential decrees and administrative regulations have significantly hampered the principles, contradicting, at least in fact, the spirit of the constitutional guarantees. In the name of public order and with the sapient use of ambiguous legislation, these limitations are increasingly frequent, and generate uncertainty and apprehension among Russia's citizens with regard to the legitimacy of certain behaviors. The principle consequence consists of the marked subservience of numerous ISPs which, while not directly targeted by governmental measures, modified their own governance to the existing overall climate of repression. In a word: self-censorship.

6.2.14.3 Relevant Events

As worrisome as this scenario may sound, the importance of *netyzdat* in stimulating democracy in Russia cannot be overlooked. The prior copy approval, the censorship, the gag laws that stifle the freedom of expression for "classic" journalists also affect, this is certain, Russian bloggers and digital dissidents as well, but at the same time there can be no doubt that the structure of the Internet makes it much more difficult to control the enormous stream of information that flows through the web. The "Internet nation" is an avid consumer of independent and anti-government materials; members of opposition parties, thinkers and journalists regularly post to blogs and opposition websites.[254]

For these individuals, for this nation, Internet represents the only discussion channel that is without state censorship, control, or moderation. Posting messages on *LiveJournal* makes sense, writes Alexei Navalny,[255] because "I, like any person, can be frightened, bribed, removed, and so on, but this should not bring our activity to a halt." If you don't have the possibility to distribute a piece of news through conventional channels, today in Russia, and the world, you can reach millions of Internet users, almost effortlessly. Consider the example of Russiabribe.ru: "If you gave a bribe or if you were extorted to give a bribe, inform us about it. We guarantee your anonymity." Once again, and as always, *collective collaboration*, the

[253] See http://www.medialaw.ru/e_pages/laws/russian/personal-data-en.htm. Accessed 19 November 2011.

[254] See, *inter alia*, *Ej.ru* (*Ezhednevnyi Zhurnal*), *Newtimes.ru*, *Grani.ru*, *Gazeta.ru*, *Kommersant.ru*, *EkhoMoskvy.ru* and *NovayaGazeta.ru*.

[255] See Anand Varghese, "*Mapping the Russian Blogosphere*" (Peace Brief No. 72, US Institute of Peace, Washington, DC, December 20, 2010).

anonymous multitude, are functioning as the only weapons in a peaceful, non-violent revolution that strives for *freedom*.

6.2.15 North Korea: The Main Digital Liberties Issues

6.2.15.1 Internet, Censorship and Surveillance in North Korea

North Korea occupies the northern portion of the Korean Peninsula, separated, since 1945, from its opponent, South Korea, by a sort of *demilitarized zone*, a 4- km wide strip of land that separates the two States. North Korea is officially a socialist republic, but in reality the government is more of a stalinist-style dictatorship, based on the *Juche* ideology of self-reliance and autonomy. The largely authoritarian policies of the government, and especially of its leader, and the nearly complete separation of the nation from the rest of the world are in fact based on this ideology and its principles, representing a fusion of neo-confucianism and stalinism. North Korea in fact is almost completely closed off to the outside world, and its government actively promotes policies of social and economic isolation. As Fitzgerald remarks, since the end of the World War Two, in addition to establishing the embargo of Cuba in 1963, the United States has imposed TWEA based economic sanctions targeted at China (1950–1971), North Korea (1950-present), North (1964–1994) and South Vietnam (1975–1994), and Cambodia (1975–1992) (Fitzgerald 1998: 16).

The country's current leader is Kim Jong-il, who, like his father, has nearly absolute power over his citizen-subjects.

North Korea is often the target of human-rights campaigns decrying the country's numerous violations of nearly all rights. Clearly, in an environment characterized by prisoners camps, torture, medical experimentation, in addition to numerous other violations of basic human rights, the freedoms of expression and of speech are practically inexistent.[256]

[256] For a preliminary overview regarding the telecommunications sector in North Korea see Noland's study concerning telecommunications policies in that country and the decision to authorize *Orascom*, a foreign cellular provider (Egyptian), to provide nationwide cellular service (Noland 2008). The author remarks that "The country faces both external and self-imposed internal constraints on telecommunications modernization, however. Externally, North Korea is one of the few remaining socialist states and the most militarized country in the world. It is embroiled in a diplomatic conflict over its nuclear ambitions. The upshot is that it is subject to *Coordinating Committee for Multilateral Export Controls* (COCOM) restrictions under the Wassenaar Agreement, impeding its ability to import state-of-the-art technology." (Noland 2008: 3). See also the interesting Nanto and Chanlette-Avery essay concerning a policy analysis of North Korea (Nanto and Chanlette-Avery 2010) and Hyang Kim's more focused article regarding the North Korea's "cyberpath" (Hyang Kim 2004). The author explains that the absence of cyber openness for IT development is a result of the leadership's political consideration of the negative impacts such openness would have on regime stability (Hyang Kim 2004: 191). Important political issues are also described in the Ko, Lee and Jang study regarding political and economic implications of the Internet in North Korea (Ko et al. 2009).

The *OpenNet Initiative* report regarding North Korea is unequivocable:

> Government restrictions on online content and connectivity render the Democratic People's Republic of Korea (North Korea) a virtual "black hole" in cyberspace. While shunning Internet accessibility and functionality, Pyongyang has opted for an isolated, domestic intranet consisting of approximately thirty Web sites approved by the government and available only to a privileged minority. […] Most Internet users […] are dependent upon Chinese service providers for connectivity - and thus are subject to China's filtering regime. […] The near absence of connectivity, even to the isolated and heavily filtered Kwangmyong intranet, is consistent with the North Korean regime's efforts to regulate all information and communication in the country. There are no independent media in North Korea. Personal radios and televisions must be modified to receive only government stations and registered with the authorities. A nationwide ban on mobile phones has also been in place since May 2004. (ONI North Korea 2007: 1, 2).

The scholar Hyang Kim observes that politics has been the main culprit thwarting development of the country's information technology industry, because the politicians are too apprehensive about the destabilizing effects the opening of the Internet and of cyberspace may have on its society (Hyang Kim 2004: 192–193). Ko notes also that the control of the Internet in North Korea is the tightest compared to that of other authoritarian countries, in that the Internet is blocked by all means available. This is principally due to concerns about expected negative effects of the Internet on the stability of the regime (Ko et al. 2009: 286). Ko also remarks that technology, although infrastructure is still poor, is not the main problem for Internet opening in North Korea. It is the Internet's potential to bring negative social effects and, more importantly, to pose a threat to the political stability of the regime that makes North Korea hesitant to open to the Internet (Ko et al. 2009: 288). According to this scholar, the issue of *regime maintenance* which makes North Korea hesitate on Internet opening is related to international relations, particularly between North Korea and the United States, including military and security issues surrounding the Korean peninsula. Ko concludes that until recently, given the worsening relations between North Korea and the United States, in particular surrounding North Korea's nuclear and missile tests, it could be expected that the Internet opening of North Korea would not happen in the foreseeable future (Ko et al. 2009: 288).

Deva provides a fascinating explanation of the relationship between North Korea and the United States regarding the freedom of the Internet in that country (Deva 2007). The author observes that under the Freedom Act, the U.S. President can designate a country as Internet-restricting if "the government of the country is directly or indirectly responsible for a systematic pattern of sub-stantial restrictions on Internet freedom during the preceding 1- year period". Although such a designation is to be made annually by the President, the Freedom Act lists certain countries, such as China, Iran, North Korea, Burma, Tunisia and Vietnam, that are to be regarded as Internet-restricting countries even without specific annual designation as such (Deva 2007: 312). The scholar remarks that the inclusion of North Korea in

this list results in a number of prohibitions, the most important of which impose trade restrictions on U.S. corporations and their overseas subsidiaries. Deva outlines five principal obligations:

1. the Act prohibits any U.S. business that provides or hosts any Internet search engine from locating within an Internet-restricting country any computer hardware which is used to house, store, serve, or maintain files or other data involved in providing such search engine. The search engine providers are also not permitted to alter search results at the request of Internet-restricting countries.
2. U.S.-based search engine providers are also obliged to provide to the Office of Global Internet Freedom a list of all terms submitted to them by Internet- restricting countries to filter search results.
3. The Act further provides that any U.S. business that maintains an Internet content hosting service shall not conduct Internet jamming of a U.S.-supported website in an Internet-restricting country.
4. U.S. corporations that maintain an Internet content hosting service must provide the Office of Global Internet Freedom with copies of all data and content that it has blocked or removed at the request of an Internet-restricting country.
5. No U.S. business that maintains an Internet content hosting service may provide to an Internet-restricting country any information that personally identifies a particular user of such content hosting service, "except for legitimate foreign law enforcement purposes as determined by the Department of Justice." (Deva 2007: 312–313).

As Beutz Land correctly remarks, North Korea, similarly to Cuba, controls Internet content by limiting access to the Internet altogether (Beutz Land 2008: 15–16).

6.2.15.2 Laws and Regulations

The primary source of statutory law in North Korea is its Constitution,[257] based upon the concept of *Juche* created by the "Eternal President", father of the country's current leader, and founder of the country itself, Kim-Il Sung.[258] The Constitution widely reflects the ideological elements of *Juche*, and, most especially the precepts of the economic and social independence of the state, thus justifying the state's nearly unlimited powers of intervention in the daily lives of the country's citizens.

[257] See the English translation of the text of the Constitution at the address http://www.servat.unibe.ch/icl/kn00000_.html. Accessed 16 October 2011.

[258] See the Preamble to the Constitution: Comrade Kim Il Sung founded the immortal Juche idea, organized and guided an anti-Japanese revolutionary struggle under its banner, created revolutionary tradition, attained the historical cause of the national liberation, built up a solid basis of construction of a sovereign and independent state in the fields of politics, economy, culture and military, and founded the DPRK.

Of note, in this regard, is Article 119 of the Constitution,[259] conferring upon the state extremely broad intervention powers in the presence of any action deemed to be in any way harmful to the interests of the state, thus granting nearly unlimited powers of *censorship*.

In reality, but unfortunately only on paper, the Constitution even provides for the protection of the rights of the country's citizens, with Article 67 expressly granting the right to the *freedom of expression*.[260]

However, with the exception of Article 67, there is no other provision, or even any other reference regarding the media or the freedom of speech or expression.

With regard to the country's law, there are two laws, approved in 2003 and 2004, that may be applied to the digital world, protecting, respectively, software[261] and the software industry[262]; the underlying motive for both clearly being a purely economically-driven desire to attract foreign investors.

6.2.15.3 Internet Availability and Laws Regarding the Media

The lack, in the North Korean legal framework, of any laws regarding the media has a very simple explanation: there are no independent forms of communication whatsoever.

Currently, the Internet is available to only a miniscule portion of the country's population, limited to top government officials and business people with commercial interests abroad. Connections to the web are established primarily via satellite link to servers in Germany, where the KCC (the state authority for computer development) has opened its specially-created European offices.

---

[259] The text of Article 119 is: "The Cabinet has duties and authority to: 1. adopt measures to execute state policy. 2. Institute, amend, and supplement regulations concerning state management based on the Constitution and departmental laws. 3. Guide the work of the Cabinet commissions, ministries, direct organs of the Cabinet, local people's committees. 4. Set up and remove direct organs of the Cabinet, main administrative economic organizations, and enterprises, and adopt measures to improve the State management structure. 5. Draft the State plan for the development of the national economy and adopt measures to put it into effect. 6. Compile the State budget and adopt measures to implement it. 7. Organize and exercise works in the fields of industry, agriculture, construction, transportation, communications, commerce, trade, land management, city management, education, science, culture, health, physical training, labor administration, environmental protection, tourism and others. 8. Adopt measures to strengthen the monetary and banking system. 9. Do inspection and control work to establish a state management order. 10. Adopt measures to maintain social order, protect State and social cooperation body's possession and interests, and to guarantee citizens' rights. 11. Conclude treaties with foreign countries, and conduct external activities. 12. Abolish decisions and directions by economic administrative organs, which run counter to the Cabinet decisions or directions".

[260] The text of Article 67 is: "1. Citizens are guaranteed freedom of speech, the press, assembly, demonstration and association. 2. The State guarantees the conditions for the free activities of democratic political parties and social organizations."

[261] *Computer Software Protection Law*, June 2003.

[262] *Software Industry Law*, June 2004.

There are also a limited number of Internet cafés, called *Internet PC Rooms*, which are connected to Chinese servers; in this case, in addition to pervasive filtering of all contents, connections are available only to a select few due to the prohibitive costs of nearly $10.00 per hour.[263]

The majority of the country's population uses a domestic intranet system created in 2002 with a fiber optic system managed by the *Korea Post and Telecommunications Corporation* under the aegis of the *Ministry of Post and Telecommunications*.

This system features chat forums and e-mail, all of which are constantly monitored, in addition a few dozen web sites chosen and monitored by the government, that exist primarily to extol the virtues of the country's leader.

The absence of any true way to access to the Internet and simultaneous need to communicate, even if in an extremely limited fashion, with the outside world, has created not a few problems uncertainty at government levels.

Kim Jong-il himself has stressed the importance of technology as a fundamental economic resource, especially in a state, such as North Korea, that aspires to complete autonomy.[264] Moreover, it is widely known that, when correctly used, the Internet can become a formidable and highly cost-effective tool for propaganda.

Therefore, for the past several years, a number of state authorities have sought to develop an Internet system that is able to, on the one hand, encourage economic development, but that, at the same time, manages to avoid free access to contents that the regimes deems unacceptable. As evidenced by recent academic reports,[265] what the North Korean government apparently would like to accomplish is what Lessig defined as the passage from *perfect control* to *effective control* (Lessig 1999), that is say, allowing access to the global network, but without relinquishing control over what is actually viewed. In order to do this, the government is seeking to reproduce China and Cuba's systems, while at the same time attempting find a solution that is better adapted to its internal policies.

---

[263] Concerning the control of Internet cafés see the brief report "Controlling Internet Cafè in North Korea" by Yang Yung, at the address http://www.dailynk.com/english/read.php?cataId=nk00300&num=206. Accessed 19 November 2011. The reporter writes: "It is known that internet connection is good for computer games and email but only connects within North Korea, and the connection does not reach to outside information".

[264] See Chen, Ko and Lee remarks regarding this statement: "The North Korean leader, Kim Jong Il, says there are three kinds of fools in the twenty-first century – people who smoke, people who don't like music, and people who don't know how to use a computer. […] Ironically, despite Kim's self-proclaimed interests in modern information technology, North Korea remains almost completely cut off from the Internet. […] The North Korean government has strategically developed its IT industry since the mid-1990s in an effort to leapfrog its economic development. The regime has subsequently built a closely monitored domestic intranet and some propaganda web sites, as well as encouraged social elites such as government officials, engineers, scientists, and university students to make use of digital technology in order to catch up with the global trend of developing virtual networks that allow people to share knowledge and exchange information. However, network access remains extremely limited in North Korea; only no more than a few thousand people in Pyongyang have direct but heavily censored access to the Internet via a pipeline through China – their main task is to plunder the web for technical information to be fed to the domestic intranet" (Chen et al. 2010: 650).

[265] See, *inter alia*, Chen et al. 2010.

Currently various projects are being developed, although to date none have been completed.

Noland, in an essay published in 2008, remarked that:

> […] North Korea is working with China to develop firewall systems that would permit less-restricted access to the World Wide Web while allowing officials to proscribe content. A German affiliate of the North Korean government computer center has reportedly also been contracted to provide such services. It is likely that private access will gradually expand subject to this firewall, perhaps with commercially oriented services in the KIC forming the leading edge. The DPRK government has a long history of engaging in varied and illicit commerce. Some have expressed concerns that as its Internet capability expands, the DPRK may become a location for servers hosting child pornography websites as a way of making money, as well as increasing its capabilities in cyberwarfare (Noland 2008: 14–15).

6.2.15.4 Censorship and Repression Activities

Censorship is nearly inexistent in North Korea, for the simple reason that the only sources of information are firmly in the hands of the government. All television and radio stations are run exclusively by the state or the *National Workers' Party*; furthermore, all privately owned televisions and devices are modified to receive only the country's governmental stations and channels.

This complete control extends to all books and newspapers available in the country as well. The only news available comes from a specially-created government authority, the *Korean Central News Agency*, whose principal duty is to praise the state and to recount the daily accomplishments of the country's leader.[266]

As mentioned above, access to the Internet is nearly absent and available to only a select few. There are almost no North Korean Internet sites accessible from outside the country, although the suffix *.kp* is used by the few state-run sites.

The country's telephone system is similarly backward. Mobile telephones have available only since 2004 and only in the capital. In the north of the country, efforts have been to use Chinese GSM SIM cards obtained on the black market in order to connect to the Chinese network (widely filtered itself).

The North Korean government is always highly alert to any such initiative and acts quickly, intervening with extremely repressive methods. Clearly, however, it is difficult to discuss the freedom of speech in a country where, according to the unanimous opinion and documentation of all humanitarian organizations having any dealings at all with North Korea, it is not even possible to speak of the existence of basic human rights.

Chen, Ko and Lee remark that:

> The main purpose for the North Korean regime to allow the Internet access is to reap the potential economic and technological benefits. Therefore, the regime is most likely to implement stringent policies when it comes to the social uses of the Internet. The constitution

[266] See the web site of the *Korean Central News Agency* at the address http://www.kcna.kp/. Accessed 19 November 2011.

> of North Korea gives the cabinet and local people's committees the authority to inspect and control any information in the name of maintaining state security, hence allowing the government to monitor all telecommunications including web activities. This means that the regime has largely adopted a 'reactive' attitude toward the Internet as a potential political threat (Chen et al. 2010: 658, 659).

The idea of *Mosquito Net* is perhaps the best example of this strategy:

> Kim Hûng-kwang, the North Korean IT scientist and defector, argues that North Korea is following a 'Mosquito-Net' model of Internet control […] Essentially, the idea of a 'Mosquito Net' entails attempts to attract the inflow of foreign investment while simultaneously blocking infiltrations of foreign ideas, news, and culture. […] Up to now, North Korea has been following the strictest kind of Internet control policy even among authoritarian regimes. It can be predicted that the regime will continue to implement tight Internet regulations even after it allows wider access to the Internet […] the Internet, and indeed, information technology in general, is a double-edged sword for the regime. It can bring enormous benefits, but the potential danger is just as great. The awareness of this dual character so far has led to the regime's halting approach to the greater use of the Internet […] Nevertheless, the nature of the Internet makes it inherently difficult for the regime to contain the spread of ideas and information. No matter how hard the regime tries to control the Internet, there will be loopholes and ways for people to bypass censor and surveillance. Moreover, once the regime weakens and loosens its grip over the society, the Internet has the potential to facilitate social movements. (Chen et al. 2010: 660, 666).

A 2008 Pentagon report, cited by Benkler (Benkler 2011) includes North Korea among those governments that have blocked access to *Wikileaks.org*-type web sites, claiming they have the right to investigate and prosecute *Wikileaks.org* and associated whistleblowers, or insisting they remove false, sensitive, or classified government information, propaganda, or malicious content from the Internet (Benkler 2011: 318).

6.3 Revolts and Digital Dissidence in Egypt and Tunisia: Where It All Began

6.3.1 A Brief Summary of Digital Dissidence in Egypt

Important events occurred in Egypt in the last years has been discussed in several portions of this book. There remain, however, some concluding reflections due to interesting peculiarity of the events occurring in this country.

In a recent study by Khamis and Vaughn (Khamis and Vaughn 2011) there is an analysis of *cyberactivism* in the egyptian revolution: long-time dictator Hosni Mubarak was forced to step down under pressure from a popular, youthful, and peaceful revolution characterized by the *instrumental use of social media*, especially *Facebook*, *Twitter*, *YouTube*, and text messaging by protesters, to bring about political change and democratic transformation. According to these scholars, main issues before, during and after those events, were:

1. *events were happening in an original political landscape*. Khamis and Vaughn write that, for a number of years, the Arabian media landscape has been witnessing a perplexing paradox in the form of a gap between the vibrant and active media arena, where many resistant and oppositional voices could be heard, and the dormant and stagnant political arena, which did not exhibit any serious signs of active change, popular participation, or true democratization (Khamis and Vaughn 2011: 2);
2. *control of the media*. Prior to 1990, the authors remark, most media ownership in the Arabian world lay with governments, and most media functioned under strict governmental supervision and control. In this era, Arabian media were mostly controlled by governments mainly to keep lay people uninformed, and thus incapable of effectively participating in political controversies and rational debates;
3. *the rise of the Internet*. New media revolution, the authors observe, erupted in the Arabian world after 1990, inspired by the introduction of both satellite television channels and the Internet, and in the 1990s Internet penetration started to spread throughout the Arab world;
4. *three important effects.* The role of new media before, during, and after the Egyptian revolution was especially important, the scholars remark, in *three intertwined ways*: (a) enabling cyberactivism, which was a major trigger for street activism, (b) encouraging civic engagement, through aiding the mobilization and organization of protests and other forms of political expression, and (c) promoting a new form of citizen journalism, which provides a platform for ordinary citizens to express themselves and document their own versions of reality;
5. *the Internet shut-down*. Once the protests began to threaten the Mubarak regime's existence, the state used a really aggressive method to impede Internet and mobile phone access. On January 28, 2011, the Egyptian government shut off the Internet and mobile phone services for the entire country, resulting in a blackout that lasted almost 1 week, and the economic impact of the Internet and mobile phone shutoff was staggering, with preliminary estimates of $90 million in losses by the Organization for Economic Cooperation and Development (OECD). The blackout, which lasted nearly a week, forced activists, the authors note, to find more innovative workaround solutions, such as setting up FTP accounts to send videos to international news organizations, or using landlines to connect to Internet services in neighboring countries by calling international numbers with older dial-up modems, a connection that was slow but sufficient for posting tweets about events on the ground. They even resorted to using Morse code, fax machines, and ham radio to get the word out about events on the ground, and the web site for the activist group *We Rebuild* transcribed transmissions from Egyptian amateur radio stations and posted resources for circumventing the blackout. They also smuggled satellite phones and satellite modems into Egypt, which did not depend on Egypt's infrastructure to function. Although most Internet connections were cut, the ISP *Noor* was working because it was used by the Egyptian stock exchange and Western companies, and many people and businesses who subscribed to *Noor* removed the passwords from their wi-fi routers so that others

could use their connection. During the Internet blackout, *Google* and *Twitter* scrambled to offer the *Speak-2-Tweet*, a service whereby users could call an international telephone number to post and hear *Twitter* messages without the Internet. The Small World Newsproject *Alive* partnered with Speak-2-Tweet to translate voice messages from protesters at Tahrir Square

6.3.2 A Brief Summary of Digital Dissidence in Tunisia

Electronic resistance activities in Tunisia were discussed in different parts of this study too, so we will just draft, in this Section, a summary of the most important issues.

The Tunisian Revolution led to the downfall of the regime of President Zine el-Abidine Ben Ali on 14 January 2011. The revolutionary process initiated the 17 December 2010, following the self-immolation of a young vegetable seller in the town of Sidi Bouzid. This event pushed together distinct dynamics: internal weakening of the regime, alienation of élites, growing popular unrest, remobilisation of youth around modern means of communication, and the survival of traditional socio-economic structures, which could serve to reinforce these dynamics.

A detailed report by the *International Crisis Group*, describing popular protests in North Africa, and identifying Tunisia as the state where it all began, outlines several fundamental points:

1. *the tradition of activism*. The country's history of political activism and social mobilisation, which decades of regime repression never fully stifled, was very important. This politically activist tradition served the nation well during the uprising, as workers, the unemployed, lawyers and members of the middle class coalesced into a broad movement;
2. *use of the technology by young people*. Satellite television channels and social networking sites – from *Facebook* to *Twitter* – helped spread the movement to young members of the middle class and elite ;
3. *radicated will of contestation*. Tangible signs of a contestation of power began to emerge on the ground in 2000. That year, the hunger strike of writer and journalist Taoufik Ben Brick, covered and publicised primarily in the European media, had shined a spotlight on the question of political freedom. In 2003, the arrests of Internet users by the authorities announced the arrival of new political and generational phenomena. This Internet phenomenon, while both generational and a harbinger of new repertoires of action, was nevertheless not born with the Sidi Bouzid revolt. In February 2003, nine youths web-surfing in southern Tunisia were arrested by the authorities and accused of terrorism. According to their lawyers, their only crime was to have visited banned web sites. The case of the "Zarzis Internauts" culminated in October 2005 with an international solidarity campaign mounted primarily in France, just 1 month before Tunis was to host the World Summit on the Information Society (WSIS);

4. *not only a Facebook effect*. If the reasons for Ben Ali's fall are clearly not limited to the "Facebook effect", and if this is not a "twitter revolution", it is necessary to understand the importance of social networks in shaping the movement. With nearly two million *Facebook* users in Tunisia, and a core group of about 2,000 active bloggers, the Internet has played a key role by giving the movement a way to achieve visibility that traditional media could not provide, by radicalising the population by posting images of the crackdown, by helping coordinate the insurrection, and, finally, by facilitating the emergence of new social actors bringing with them their own political culture;
5. *circumvention of censorship*. Facing a media landscape characterised by heavy censorship throughout the decade of the 2000s, Tunisians developed political and informational web sites in the form of individual or collective blogs, such as *Nawaat*, Tune-zine, or Réveil tunisien. Tunisian cyberspace politicised gradually, under the double threat of online censorship and arrests of Internet activists: sll sites, whether for cooking, sports, fashion or online dating, began to carry messages that conveyed political content. At first, they were divided between ideological tendencies, but very soon censorship brought them together rather than polarising them. *Facebook* became a place to criticise dictatorship, corruption, and censorship – in short a place to challenge the regime;
6. *facilization of the protes*. Tunisia's online activists admit that Internet-based networks did not immediately contribute to the dynamics of the Tunisian uprising. However, it was *Facebook* that enabled a political connection between labour activists of central Tunisia and middle class youth across the nation and facilitated organisation of the protests in Tunis just prior to the fall of Ben Ali;
7. *combination of technological means*. *Facebook* combined with *YouTube*, a video-uploading and sharing web site, facilitated the diffusion of images of the insurrection. Some Tunis-based bloggers travelled to provincial towns to collect images of the protests, often using mobile phones, and sent them to international television stations, particularly France24 and Al-Jazeera.

References

AFP. 2012. Cartel web presence could be used against them. http://news.asiaone.com/News/Latest%2BNews/World/Story/A1Story20120531-349519.html. Accessed 10 June 2012.

Amnesty International. 2010. Report: Restrictions of freedom of expression in Cuba. http://www.amnesty.org/en/library/asset/AMR25/005/2010/en/62b9caf8-8407-4a08-90bb-b5e8339634fe/amr250052010en.pdf. Accessed 26 Sept 2011.

Anh Tuân, Nguyên. 2007. From VietNet to VietNamNet: Ten years of electronic media in Vietnam. http://www.hks.harvard.edu/presspol/publications/papers/discussion_papers/d43_nguyen.pdf. Accessed 15 Nov 2011.

Ariffin, L.J. 2012. Rais backs Dr M call for curbs to Internet freedom. http://my.news.yahoo.com/rais-backs-dr-m-call-for-curbs-to-065031693.html. Accessed 10 June 2012.

Bambauer, Derek E. 2008. Filtering in Oz: Australia's foray into Internet censorship. http://ssrn.com/abstract=1319466. Accessed 20 Nov 2011.

Benkler, Yochai. 2011. A free irresponsibile press: Wikileaks and the battle over the soul of the networked fourth estate. *Harvard Civil Rights-Civil Liberties Law Review* 46: 311–397. http://www.benkler.org/Benkler_Wikileaks_current.pdf. Accessed 14 Nov 2011.

Beutz Land, Molly. 2008. Protecting rights online. http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1295448. Accessed 14 Nov 2011.

Boas, Taylor C. 2000. The dictator's dilemma? The Internet and U.S. policy toward Cuba. *The Washington Quarterly* 23(3): 57–67.

Bowman, Gregory W. 2004. E-mails, servers, and software: U.S. export controls for the modern era. *Georgetown Journal of International Law* 35: 319–378.

Burleigh, M. 2012. Iran to crack down on web censor-beating software. http://phys.org/news/2012-06-iran-web-censor-beating-software.html. Accessed 10 June 2012.

Burns, Alex, and Ben Eltham. 2009. Twitter free Iran: An evaluation of twitter's role in public diplomacy and information operations in Iran's 2009 election crisis. http://vuir.vu.edu.au/15230/1/CPRF09BurnsEltham.pdf. Accessed 19 Nov 2011.

Butt, Danny (ed.). 2005. Internet governance. Asia-Pacific perspectives. New Delhi: Elsevier. http://www.apdip.net/publications/ict4d/igovperspectives.pdf. Accessed 23 Nov 2011.

Cason, James C. 2003. The human rights situation in present-day Cuba. *Human Rights Review* 2003: 46–55.

Cavoukian, Ann. 2011. Ontario's privacy commissioner on the online spying bills. http://openmedia.ca/blog/ontarios-privacy-commissioner-online-spying-bills. Accessed 23 Nov 2011.

Chen, Cheng, Kyungim Ko, and Ji-Yong Lee. 2010. North Korea's Internet strategy and its political implications. *The Pacific Review* 23(5): 649–670.

Chin, J. 2012. Talk of Tiananmen muzzled on Chinese web. http://online.wsj.com/article/SB10001424052702303506404577445901268141694.html. Accessed 10 June 2012.

Chowdhury, Mridul. 2008. The role of the Internet in Burma's saffron revolution. http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1537703. Accessed 23 Oct 2011.

CSG Cuba Study Group. 2010. Empowering the Cuban people through access to technology. http://www.cubastudygroup.org/index.cfm/empowering-cubans-through-technology. Accessed 23 Oct 2011.

Dacanay, Nikos. 2010. Internet centers/usage by Burmese ethnic migrants in Mae Sod: Traversing the borders of Internet divide and recasting ethnic identities. http://www.upf.edu/amymahan/_pdf/Paper_for_ICTD4_Conference_October_30_2010.pdf. Accessed 23 Oct 2011.

Danitz, Tiffany, and Warren P. Strobel. 2001. Networking dissent: Cyber activists use the Internet to promote democracy in Burma. In *Networks and Netwars: The future of terror, crime, and militancy*, ed. John Arquilla and David Ronfeldt, 129–169. Santa Monica: Rand Corporation.

Deibert, Ronald, John Palfrey, Rafal Rohozinski, and Jonathan Zittrain. 2012. *Access contested. Security, identity, and resistance in Asian cyberspace*. Cambridge/London: The MIT Press.

Del Riego, A., and Adrianna C. Rodriguez. 2011. Ladies in white: The peaceful march against repression in Cuba and online. *Harvard Human Rights Journal* 24(1): 221–240.

Deva, Surya. 2007. Corporate complicity in Internet censorship in China: Who cares for the global compact or the global online freedom act? http://papers.ssrn.com/sol3/papers.cfm?abstract_id=964478. Accessed 13 Nov 2011.

Duncombe, Constance. 2010. The twitter revolution? Social media, representation and crisis in Iran and Libya. http://law.anu.edu.au/coast/events/apsa/papers/151.pdf. Accessed 13 Nov 2011.

Fitzgerald, Peter L. 1998. Pierre goes online. Blacklisting and secondary boycotts in U.S. trade policy. *Vanderbilt Journal of Transnational Law* 31: 1–96.

Freedom House. 2011. Report: Freedom on the Net 2011. Cuba. http://www.freedomhouse.org/images/File/FotN/Cuba2011.pdf. Accessed 26 Sept 2011.

Goldstein, Joshua. 2007. The role of digital networked technologies in the Ukrainian orange revolution. http://cyber.law.harvard.edu/sites/cyber.law.harvard.edu/files/Goldstein_Ukraine_2007.pdf. Accessed 10 Nov 2011.

Gómez, R. 2008. The role of blogs in breaking the media's embargo and telling the truth about Cuba: Comment. http://www.ascecuba.org/publications/proceedings/volume18/pdfs/henrygomez.pdf. Accessed 26 Sept 2011.

Gong, Rachel. 2011. Internet politics and state media control: Candidate weblogs in Malaysia. *Sociological Perspectives* 54(3): 307–328.

Henken, Ted. 2011. The Internet and emergent blogosphere in Cuba: Downloading democracy, booting up development, or planting the virus of dissidence and destabilization? http://www.ascecuba.org/publications/proceedings/volume20/pdfs/henken.pdf. Accessed 23 Oct 2011.

Hill, David T. 2002. East Timor and the Internet: Global political leverage in/on Indonesia. *Indonesia* 73: 25–51.

Hoffmann, Bert. 2011. Civil society 2.0?: How the Internet changes state-society relations in authoritarian regimes: The case of Cuba. http://www.isn.ethz.ch/isn/Digital-Library/Publications/Detail/?lng=en&id=126011. Accessed 23 Oct 2011.

HRW Human Rights Watch. 2012. Thailand: Internet trial a major setback for free speech. http://www.hrw.org/news/2012/05/30/thailand-internet-trial-major-setback-free-speech. Accessed 12 June 2012.

Hyang Kim, Yoo. 2004. North Korea's cyberpath. *Asian Perspectives* 2004 28(3): 191–209. Online at the address http://www.asianperspective.org/articles/v28n3-h.pdf. Accessed 19 Nov 2011.

Jacobi, Emily. 2011. Burma: A modern anomaly. In *Mobile technologies for conflict management. Online dispute resolution, governance, participation*, ed. Marta Poblet, 141–157. Dordrecht/Heidelberg/London/New York: Springer.

Kee, J. 2012. Bad laws won't stop cyber crime. http://www.loyarburok.com/2012/05/28/bad-laws-stop-cyber-crime/. Accessed 10 June 2012.

Kitzberger, Philip. 2010. The media activism of Latin America's leftist governments: Does ideology matter? http://www.giga-hamburg.de/dl/download.php?d=/content/publikationen/pdf/wp151_kitzberger.pdf. Accessed 20 Nov 2011.

Ko, Kyungmi, Heejin Lee, and Seungkwon Jang. 2009. The Internet dilemma and control policy: Political and economic implications of the Internet in North Korea. The Korean journal of defense analysis 21(3): 279–295. Online at the address http://kida.re.kr/data/kjda/RKJD_A_408893_P.pdf. Accessed 19 Nov 2011.

Lam, Dieu, Jonathan Boymal, and Bill Martin. 2004. Internet diffusion in Vietnam. *Technology in Society* 26: 39–50.

Lessig, Lawrence. 1999. *Code and other laws of cyberspace*. New York: Basic Books.

MacKinnon, R. 2012. Google confronts the Great Firewall. http://www.foreignpolicy.com/articles/2012/05/31/google_confronts_china_again. Accessed 12 June 2012.

MANISAR, D. 2006. Freedom of information around the world. http://www.freedominfo.org/wp-content/uploads/documents/global_survey2006.pdf

Masnick, M. 2012. Google cryptically alerts the world that it will nudge Chinese searchers away from censorship. http://www.techdirt.com/articles/20120602/02512019184/google-cryptically-alerts-world-that-it-will-nudge-chinese-searchers-away-censorship.shtml. Accessed 11 June 2011.

Moon, Richard. 2008. Report to the Canadian human rights commission concerning Section 13 of the Canadian human rights act and the regulation of hate speech on the Internet. http://www.chrc-ccdp.ca/pdf/moon_report_en.pdf. Accessed 20 Nov 2011.

Mottaz, Laura. 2010. New media in closed societies: The role of digital technologies in Burma's saffron revolution. Democracy and Society, 7.2. http://www.democracyandsociety.com/blog/wp-content/uploads/2010/07/MottazSaffronRevolution7.22.pdf. Accessed 23 Oct 2011.

Nanto, Dick K., and Emma Chanlette-Avery. 2010. North Korea: Economic leverage and policy analysis. http://www.fas.org/sgp/crs/row/RL32493.pdf. Accessed 19 Nov 2011.

Nguyen, Tuyen Thanh, and Don Schauder. 2007. Grounding e-government in Vietnam: From antecedents to responsive government services. http://www.jbsge.vu.edu.au/issues/vol02no3/Nguyen.pdf. Accessed 15 Nov 2011.

Niyazova, Umida. 2008. The absence of free and independent mass media and the total destruction of freedom of speech in Uzbekistan. http://lib.ohchr.org/HRBodies/UPR/Documents/Session3/UZ/CEJU_UZB_UPR_S3_2008_CentreofExtremeJournalisminUzbekistan_ENG_uprsubmission.pdf. Accessed 23 Oct 2011.

Noland, Marcus. 2008. Telecommunications in North Korea: Has Orascom made the connection? http://www.iie.com/publications/papers/noland1208.pdf. Accessed 19 Nov 2011.

Nordahl, Jade Josefine. 2009. Waves of democracy. Contemporary exile journalism: A case study of the democratic voice of Burma. https://www.uio.no/english/research/interfaculty-research-areas/culcom/publications/master/2010/nordahl.html. Accessed 23 Oct 2011.

OpenNet Initiative, Cuba Country Profile. 2007. http://opennet.net/research/profiles/cuba. Accessed 26 Sept 2011.

Otero, Gerardo, and Janice O'Bryan. 2002. Cuba in transition? The civil sphere's challenge to the castro regime. *Latin American Politics and Society* 44(4): 29–57.

Pelsinger, Shawn. 2010. Liberia's long tail: How web 2.0 is changing and challenging truth commissions. *Human Rights Law Review* 10(4): 730–748.

Randall, Jesse. 1996. Of cracks and crackdown: Five translations of recent Internet postings. *Indonesia* 62: 37–51.

Rodan, Garry. 1998. The Internet and political control in Singapore. *Political Science Quarterly* 113(1): 63–89.

RWB. 2011. Internet enemies report by reporters without borders. http://12mars.rsf.org/i/Internet_Enemies.pdf. Accessed 24 Oct 2011.

Sahar Khamis and Katherine Vaughn. 2011. Cyberactivism in the Egyptian revolution: How civic engagement and citizen journalism tilted the balance. Arab Media and Society. Summer 2011. Issue 13. http://www.arabmediasociety.com/?article=769

Smart, Jason, Kyle Tedeschi, Daniel Meakins, Peter Hannay, and Christopher Bolan. 2008. Subverting national Internet censorship – An investigation into existing tools and techniques. http://openduck.com/2008/12/01/paper-subverting-national-internet-censorship-an-investigation-into-existing-tools-and-techniques/. Accessed 20 Nov 2011.

Sohrabi-Haghighat, M. Hadi, and Shohre Mansouri. 2010. 'Where is my Vote?" ICT politics in the aftermath of Iran's presidential election. *International Journal of Emerging Technologies and Society* 8(1): 24–41.

Sutter, J.D. 2012. The woman who defied Saudi's driving ban and put it on YouTube. http://edition.cnn.com/2012/06/10/world/meast/sharif-saudi-women-drive/index.html. Accessed 10 June 2012.

Symmes, Patrick. 1998. Che is dead. http://www.wired.com/wired/archive/6.02/cuba.html. Accessed 24 Nov 2011.

Tamayo, J.O. 2012. Yoani Sanchez files demand against Cuban Interior Minister. http://www.miamiherald.com/2012/05/31/2826570/yoani-sanchez-files-demand-against.html. Accessed 12 June 2012.

Thiha, Amara. 2010. Revolution through cyberspace: Burmese blogosphere and saffron revolution. http://www.gg.rhul.ac.uk/ict4d/ictd2010/posters/ICTD2010%20Thiha.pdf. Accessed 23 Oct 2011.

Travaglione, Karina. 2009. Internet censorship in Australia – A 'clean-feed'? http://www.mannkal.org/downloads/scholars/internet-censorship-in-australia.pdf. Accessed 15 Nov 2011.

UNYA. 2008. United Nations youth association of Australia Internet censorship blue paper. http://unyouth.org.au/assets/Documents/bluepapers/Blue-Paper-Censorship.pdf. Accessed 18 Nov 2011.

Vedres, Balázs, László Bruszt, and David Stark. 2005. Organizing technologies: Genre forms of online civic association in Eastern Europe. *Annals of the American Academy of Political and Social Science* 597: 171–188.

Venegas, C. 2010. *Digital dilemmas. The state, the individual, and digital media in Cuba*. New Brunswick/London: Rutgers University Press.

Li, Weiping. 2012. Taiwan: Facebook's deactivation of user accounts triggered free speech concerns. http://advocacy.globalvoicesonline.org/2012/06/08/taiwan-facebooks-deactivation-of-user-accounts-triggered-free-speech-concerns/. Accessed 10 June 2012.

Weissman, C.G. 2012. Google shifts policy toward state-sponsored intrusion. http://blogs.law.harvard.edu/herdict/2012/06/08/google-shifts-policy-toward-state-sponsored-intrusion/. Accessed 10 June 2012.

Chapter 7
Conclusions: The Landscape of Digital Liberties and the Future

7.1 Human Rights in the Digital Era and the Role of Law

For the legal scholar, drawing firm conclusions with regard to (i) the *relationships* between Internet and the state of human rights, (ii) their *protection* in the digital environment, (iii) the national and international *legal frameworks* that regulate both human rights and the digital world, (iv) the level of *repression* of liberties in the world, and (v) the *technologies* used by dissidents, independent media and political opposition to circumvent limitations, is not at easy, especially in an environment so prone to rapid change and swift development.

First, and most striking, is that the extension of human rights to the Internet is of *far greater importance* among common users, activist associations and scholars than what might be perceived from an examination of the concrete legislation emanated at national levels worldwide.

Some principles, as we have seen,[1] have been established by various international Conventions, Treaties, Declarations, Recommendations, Reports, and alerts, but in the concrete legal framework of each individual country, there is a clear tendency to *repress* rather than to *liberate* technology.

From the point of view of general (formal) protection, it is possible to say that the mission has been accomplished: for a numbers of years now, the importance of the Internet for the development of human rights, of its protection and the protection of its users, has been recognized at the highest international levels. But yet, when these general principles must be activated at the national level, the trend is *brusquely interrupted*.

This the principal reason for which it appears that the path to the recognition toward the truly free use of technology will be increasingly arduous: national governments nearly always tend to shy away from technological evolution, from the

[1] See Chap. 4.

G. Ziccardi, *Resistance, Liberation Technology and Human Rights in the Digital Age*, Law, Governance and Technology Series 7,
DOI 10.1007/978-94-007-5276-4_7, © Springer Netherlands 2013

possibilities of allowing their citizens to communicate freely, to uncover secrets, to take away that advantage, held by those in power, based on discretionary powers, state secrets, and stealth.

Even in contexts considered to be far more liberal, if the legal scholar carefully analyzes the spirit underlying the norms and laws proposed, a repressive and censorial tendency nearly emerges, not only in those nations where these phenomena are plainly evident, but also in those with far more stable political environments.

Consider, purely as an example, that the obligation to register all blogs (with a state "entity" that can monitor them, with the clear aim of limiting the freedom of speech of the blogger) is a heated topic even in several European countries, including Italy, where a number of bills have been proposed to do just that.[2] The requirement to register blogs as newspapers is nearly always proposed not in order to extend any journalistic protection to blogs (constitutional limits to the seizure of the printed materials, the right to criticism and satire, a sort of protection under the "umbrella" of free speech), but merely to exert *further control*.

In our analysis, this weakening of digital freedoms and rights did not regard only laws and bills commonly deemed *repressive*, but even involved legislation *to the contrary*, including laws, regulations and rulings purportedly seeking to *promote* the freedom of communication and to foster enterprise and incentive plans. Of course, as the reader may have noticed during the course of this book, this latter type of legislation is insignificant when compared to the former.

This does not mean that it is not necessary, for observers of these matters, to constantly bear in mind the *role of law* in similar contexts, and in situations of open conflict. As Pattaro and Sartor already so perceptively wrote, more than 10 years ago, in regard to the relationships between Internet and the law, and the contrast between law and freedom (emphasis mine):

> So, on the one hand the Internet seems to *refuse law and politics*, as antiquated impediments to its creativity, as authoritarian obstacles to new and better forms of (self-)governance; on the other hand *it asks for legal solutions* (and different voices are often asking for very different legal solutions) for the new "political" problems brought about by this very creativity, problems for which a shared and consented outcomes, voluntarily adopted and even implemented by everybody within the Internet community, seems to be out of reach. […] Normative beliefs, beliefs and something has to be done, when appropriate circumstances obtain, are an essential component of social organisation. However, the law is a mix of norms and force: it is a cluster of beliefs eventually enforced by organised power. Enforcement is (unfortunately) necessary since we may have different normative beliefs, and anyway we may give priority to our individual interests over our normative beliefs: unless one body or rules (hopefully good ones) are enforced, chaos is inevitable. Therefore, the need of enforcement puts the idea of the law of cyberspace into a dilemma. If cyberlaw is going to be enforced through organised power, than it will become law, with the authoritarian aspects which characterise any type of law. The idea that "no policy is established without the unanimous approval of the denizens", *needs to be substituted with the complexities of political processes*. If cyberlaw

[2] I refer to the Italian draft law "Levi", proposed on 3 August 2007 by the deputy Ricardo Franco Levi, and then dismissed, which included a mandatory registration of all "editorial products", blogs included. See the Italian text of the draft law at the address http://download.repubblica.it/pdf/2007/legge_editoria.pdf. Accessed 23 November 2011.

> is not going to be enforced then it will be disregarded by individuals and - notice - by States and other agencies who are endowed with organised power: namely, mafia, terrorism, and dealers of children, women and men. In conclusion we must not be illuded that the novelties introduced by the Information Society may avoid the thousand and thousand-year-old problem of the relationship, better of the contrast, *between law and freedom*: also in cyberspace law (norms supported by organised force) on the one hand, may be may encroach upon freedom, on the other hand, is freedom's necessary precondition. The illusion that cyberlaw may not need the support of organised force illusion has a name: *utopia*, which means nowhere, in no place at all, neither in cyberspace you may have freedom without law, namely without organised power (Pattaro and Sartor 2002: 3–5).

7.2 Technology as an *Antibody*

I find this seemingly overpowering, and by now widely diffused, desire (to say nothing of the willingness) to control the Internet to be extremely alarming. Not only because this results in exceedingly low levels of protection of human rights in the digital era (and these levels appear destined to descend even further), but also because it is becoming more and more apparent that this approach can only lead to an unending struggle.

Technologies and their users behave like a sort of *antibody*, constantly adapting to new attempts of government censorship, continually evolving to seek out new ways to circumvent such provisions.

In all likelihood, in the future, legally established sanctions (in terms of imprisonment) will be increasingly rigid, in an attempt to discourage digital "crimes", becoming increasingly disproportionate, with respect to the perception of the same by the common citizens, and will almost inevitably inhibit further development.

As this book goes to print, no nation, as yet, has had the courage to create a body of laws clearly establishing *the freedom of Internet* and of the exchange of information (although, as mentioned in the previous chapter,[3] there are a number of very interesting current proposals before the Parliament in Iceland).

At this point, there is a second, equally important analysis, which must seek to bring together dozens of nations, all with diverse legal, cultural, religious traditions, and to categorize the differing approaches to repressive Internet control, with the objective of facilitating their comprehension, and, perhaps, 1 day, their attenuation, if not their complete elimination.

While such an analysis might at first seem nearly impossible, given the many differing contexts, approaches, histories and cultures, in fact it is simpler than one might think, given that, as has emerged during the course of this work, often the various countries in a given geographical region tend to adopt noticeably *similar strategies* (certain states taking example from their neighbors, or from those with which have good economic, political or cultural relations).

[3] See Sect. 6.2.12.

Thus approaches to repression, on a worldwide level, may in fact be divides into *three* different categories, based upon the *forms* they take:

1. *generic laws*, i.e. the use of existing laws and regulations to control the Internet;
2. *technology for control*, i.e. significant technology investments in order to exert control over the Internet;
3. *specific laws*, i.e. the use of special laws created specifically to repress the digital world.

In the first category are all those nations already having a legal and political tradition perfectly suited to the repression of any new forms of protest, or of the use of technology for the purposes of freedom, and that may, for example, make use of already existing state or government controlled media and communication systems, vague press laws which may be used for repression, laws and regulations disciplining dissent, protests, demonstrations, strikes and meeting, but also certain procedural guarantees (preventive detention, interrogation, access to defense counsel), or their absence, all factors that facilitate the creation of a generally repressive environment even in the absence of laws pertaining specifically to the Internet.

The second point regards those states having the good fortune to be in the position to rely on ample budgets consenting far-reaching societal control, only some of which are purely based on technology. These nations often purchase innovative content filtering systems from abroad, additionally paying top salaries to individual "human" monitors to listen to conversations and read messages, installing filtering systems in schools and disbursing untold amounts to technicians to conduct denial-of-service attacks against undesirable sites or cyber-wars.

The third classification involves those states which have created a special body of laws to regulate, or to stifle, the Internet. In these contexts, the effect is far worse, and determined behaviors and technologies are targeted, generally with any sanctions increased when technology or electronic media are involved.

This framework defines a situation which, from certain perspectives, is both surreal and frighteningly hierarchical.

At the top levels is the European Union with its Recommendations, Directives and proposals, leaders of leading nations in their declarations and speeches, and international Conventions which, for years, have established the protection of human rights, including on the Internet, and the fundamental importance of protecting this *medium*. However, as soon we descend by even one level, it is immediately apparent that at the more concrete, national levels not only this tendency is not maintained, but precisely opposite tendencies are far more common.

The grand, general principles are left at the wayside, unapplied, while repressive governments proceed with strict and far more oppressive legislation and regulations. This type of regulation is often presented as "in order to establish a generally free environment, we regulate those minimal aspects to maintain a civil co-existence" but, in fact, the general ideas of liberty are superseded by a truly repressive grid of laws and regulations.

7.3 The Technological Scenario

If the worldwide legal context surrounding these issues is multiform, and generally geared to repression, thus creating particular problems for the researcher, it is also true that the technological scenario also raises far more questions that can be easily answered.

See, for example, nine typical risks of information and communication technology, as Sartor clearly explained:

1. *surveillance*. The first risk is Orwell's nightmare, the use of technology for surveillance (Sartor 2010: 5);
2. *control*. The second risk is Kafka's nightmare, the use of technologies for cover control and judgment (Sartor 2010: 6);
3. *discrimination*. The third risk is Huxley's nightmare, the use of technologies for discrimination and exclusion (Sartor 2010: 6);
4. *ignorance and indifference*. The fourth risk is Bradbury's nightmare, technologies causing ignorance and indifference (Sartor 2010: 7);
5. *dependance from the machine*. The fifth risk is to lose our ability to think and act on our own, become completely passive, mere *desire machine*, relying on machines for all productive and communicative initiatives (Sartor 2010: 7);
6. *loss of communication between humans*. Sartor reserves the name of Asimov's nightmare for the sixth risk, technologies causing separation and loss of communication between humans (Sartor 2010: 8);
7. *artificial pleasure*. The seventh risk is Nozick's nightmare, technologies for illusion and artificial pleasure (Sartor 2010: 8);
8. *class division*. The eighth risk is Vonnegut's nightmare, technologies causing class division and exclusion (Sartor 2010: 9);
9. *war*. The ninth risk is Dick's nightmare, information and communication technologies for war and human destruction (Sartor 2010: 9)

Moving from Sartor's approach, there are essentially two main issues: on the one hand, (i) the ability of technology to *change society*, due to the increased diffusion of knowledge and the transparency it so often brings, and, on the other hand, (ii) the abilities of digital resistance to *resist censorship*, whether these technologies can be viewed as *technologies for liberation*, and the affinity of these activities with hacker environments.

The first point has been much debated. Positions range from quite extreme (technology leads to revolution/technology is only marginally significant to revolutionary processes) to more moderate interpretations. In my opinion, today technology is an *essential part* of opposition, revolutionary and liberation movements. The degree of importance will, of course, *vary* from country to country, but in every context technology facilitates something extremely important, that being individual communication, the ability to meet and to circulate information, both within and beyond the borders of a given society. The social capacities of new technologies become fundamental in those contexts where an act of rebellion often requires awareness of

the existence of others who share and understand one's beliefs and problems, and who are equally willing to act in pursuit of the same ideas. The ability to organize rapidly, almost instantly, thanks to *Twitter* and *Facebook* messages is, in my opinion, the single most important aspect.

The second point is the use of technology as a tool against filters and censorship and, often with the use of explicit images and videos, against those who seek to conceal or veil events occurring in a given country. This permits both the possibility for *increased responsibility* on the part of foreign countries, and for *local testimony* when all other communication channels have collapsed.

7.4 The Relationships Between Hacking and Digital Resistance

I also find fascinating the relationship between the most noble tradition of hacking, the creative use of technology to overcome concrete obstacles which present new challenges, the evolution of digital resistance activities and the principles underlying these movements.

Today, new technologies provide incredibly powerful means to facilitate and foster protest and activism movements. Digital tools can assist activists in registering and processing data, allowing greater cooperation, support and collaboration, even across distances spanning thousands of miles. Joyce, correctly, refers to six fundamental aspects of the use of available technology as a *resistance tool*:

1. *knowledge and testimony*. The first step in confronting injustice is *knowing*, and making it known, that it exists: *recording proof* of the violation of human rights, or of an episode of the abuse of power, is something that digital technologies are able to do very well (Joyce 2009);
2. *process of the information*. These *records* are not always, in and of themselves, ready to be used for political ends or for activism. At times it is necessary to *process* this information, using new technologies, so that it is more effective as proof of misdeeds or misdoings (Joyce 2009);
3. *revelation*. Another action which is embraced most enthusiastically by activists worldwide using technological tools is the *revelation* of compromising secrets and events (Joyce 2009);
4. *co-creation*. Then, there is the activity of *co-creation*: creating something together, by cooperating, is in modern times really easy thanks to wiki and blog platforms (Joyce 2009);
5. *call for action*. There is, then, the necessity to formulate a specific and concrete *request for action* to the potential activists, using the most effective technological means (Joyce 2009);
6. *aggregation*. In the grand tradition of activism worldwide, in all likelihood, the most fascinating capability of activism movements is their ability to *aggregate* people, to unite minds and skills for common events or projects. And the "mothers" of all aggregators are the blog, *Twitter* and *Facebook* (Joyce 2009).

What is it that binds the tradition of hacking to all of these technological movements? Mistrust of authority, non-acceptance of secrecy, the creative use of even those technologies considered to be obsolete, a firm belief in the *Do-It-Yourself* approach, a mix between individualism and cooperation, the support of dissidents by hacker groups which send them specifically designed tools to circumvent censorship programs.

This incredibly complex framework, consisting, on the one hand, of legal systems apparently set in place to protect human rights but that, in reality, at local levels, are actually quite repressive, and, on the other, technology that is increasingly suited to protest, oppose, and resist, providing a new era for the ideas of those early hackers, is leaving an indelible mark on our modern age, and this framework is increasingly intertwined with political movements and social upheavals which are transforming the worldwide political and social arenas.

In 2012, the scholar Yochai Benkler defended the presence of hacktivism and hacker groups like *Anonymous* in the political scenario (Benkler 2012). The scholar wrote:

> Seeing Anonymous primarily as a cybersecurity threat is like analyzing the breadth of the antiwar movement and 1960s counterculture by focusing only on the Weathermen. Anonymous is not an organization. It is an idea, a zeitgeist, coupled with a set of social and technical practices. Diffuse and leaderless, its driving force is "lulz" -- irreverence, playfulness, and spectacle. It is also a protest movement, inspiring action both on and off the Internet, that seeks to contest the abuse of power by governments and corporations and promote transparency in politics and business. Just as the antiwar movement had its bomb-throwing radicals, online hacktivists organizing under the banner of Anonymous sometimes cross the boundaries of legitimate protest. But a fearful overreaction to Anonymous poses a greater threat to freedom of expression, creativity, and innovation than any threat posed by the disruptions themselves. (Benkler 2012).

As the early hackers foresaw,[4] computers and technology have indeed changed the world, and rendered every single one of us more powerful and more able to participate in every aspect and at every level of government.

Moving ahead from the present, and seeking to envisage the future is, for the legal observer, a truly fascinating challenge: never before, having a keen understanding of the past, and sharp ability to foresee the future, has been so important.

References

Benkler, Yochai. 2012. Hacks of Valor. Why anonymous is not a threat to national security. http://www.foreignaffairs.com/articles/137382/yochai-benkler/hacks-of-valor. Accessed 16 June 2012.

Joyce, Mary. 2009. An introduction to digital activism. http://www.slideshare.net/MaryCJoyce/introduction-to-digital-activism. Accessed 23 Nov 2011.

Pattaro, Enrico, and Giovanni Sartor. 2002. Norms, laws and the internet. http://www.ieid.org/congreso/ponencias/sartorpattaro.pdf. Accessed 14 Nov 2011.

Sartor, Giovanni. 2010. Human rights and the future of the information society. http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1707724. Accessed 3 Sep 2012.

[4] See Sect. 1.1.

Author Index

G. Ziccardi, *Resistance, Liberation Technology and Human Rights in the Digital Age*, Law, Governance and Technology Series 7,
DOI 10.1007/978-94-007-5276-4, © Springer Netherlands 2013

Subject Index

G. Ziccardi, *Resistance, Liberation Technology and Human Rights in the Digital Age*, Law, Governance and Technology Series 7,
DOI 10.1007/978-94-007-5276-4, © Springer Netherlands 2013