International Journal of Information Technology and Business Management

29th September 2012. Vol.5 No.1

ISSN 2304-0777 www.jitbm.com

INTERNET AND CONTROL SOCIETY AFTER 9/11

* Dr. Murat AKTAS, Vice President of Public Administration Department of School of Economics and Administrative Sciences at Mus Alparslan University,

e-mail: aktasmurat49@hotmail.com.

Abstract: The 9/11has brought many important changes to the global political landscape. The agreement between the European Commission and U.S.A federal authorities following September 11 has given the possibility to deliver personal information to the U.S authorities without the consent of the persons concerned. Thus, the legal basis of monitoring was crafted and the world has moved to a monitoring and control society. In fact, with the development of new information and communication technologies, the traditional techniques of close surveillance has been replaced by a large electronic monitoring device, comprising a variety of methods: CCTV, wiretapping, satellite images, data etc. This paper aims to study particularly monitoring by Internet, control society and democracy after 9/11.

Keywords: Internet, monitoring, democracy and control society

.

Introduction

The terrorist attacks of September 11, 2001 have changed many things not only in the history of communication but also in the everyday life of people almost all over the world. The priority given to the fight against terrorism and cybercrime tends to shatter the legal constituted for years in order to protect citizens against threats to their freedom. The September 11 attacks have strengthened the willingness of the authorities to control the flow of information on the Web. Indeed, the supposed terrorists use the Internet to prepare attacks led the U.S. government to take a series of measures to increase flexibility and opportunities for online monitoring.

Thus the 9/11 events have opened a new period in the history. The previous period, which began with the fall of the Berlin Wall, was marked by the celebration of three major values: the democracy, rule of law and human rights. However, since the terrorist attacks against the World Trade Center, in September 11, 2001 many measures taken in the United States and in Europe (in the name of the fight against terrorism) suggest that the need for security premium now on all others. Nowadays, everyone who talks about the security points out as well the surveillance.

Conceptually, “surveillance” can be viewed from different perspectives. In the context of this paper, surveillance is explained as the police activity of gathering information on individuals. First, it includes human and technological gazing where officials watch the physical movements and activities of persons.

29th September 2012. Vol.5 No.1

ISSN 2304-0777 www.jitbm.com

Second, surveillance involves the acquisition of personal data. This includes the collection of biographical, biometric, or transactional data on individuals harvested from personal communications, electronic transactions, identifiers, records, or other documents. In the former, observations can be used for identification or may act to advance an investigation as a component of a larger body of evidence, as in the case of CCTV data. The latter involves voice or documentary information that can be used in criminal investigations or prosecutions. Hence, the meaning given to police surveillance here is the collective action of official gathering of information on persons for the stated purpose of preventing crime and terrorism or prosecuting offenders. As the police gather more personal information through surveillance, search, and seizure, a greater number of persons come within their official purview vis-à-vis suspicion profiles, threat assessments, or specific investigations (Bloss).

It is clear that the misuse of surveillance technologies creates a major twist in the exercise of at least two of our fundamental freedoms: freedom of movement and the private life. For example the agreement between the European Commission and U.S. federal authorities stating that certain personal information (name, surname, age, address, passport and credit card number, health and food preferences, previous trips, etc…) of people preparing to travel to U.S will be delivered to US custom houses without the consent of the persons concerned. Accession of people considered "dangerous" can be denied to the plane.

In fact, with the development of new technologies of information and communication, the traditional techniques of close surveillance are replaced by a large electronic monitoring device, comprising a variety of methods: CCTV, wiretapping, satellite images, electronic identity cards or passports, data etc…This study aims to analyze and understand the legal surveillance over the Internet and highlighting developments emerged since September11, 2001. However, to understand the issues and challenges of such device, you need to put it in the global environment which the philosopher Gilles Deleuze called "control society". According to him we are moving toward control societies that no longer operate by confining people but through continuous control and instant communication. (Deleuze, 1995: 174)

1. THE CONTROL SOCIETY

Traceability and transparency: these seem to be the watchwords of our time. But it is actually much transparency opaque it is because citizens, now all that can be monitored, have few means to control turn the supervision to which they are subject. Thus, the control society announced by Gilles Deleuze introduces itself as a world of traceability. The Internet is a perfect tool for this universe. Deleuze describes how the institutions of the modern disciplinary society wither and are replaced with a new kind of control that is no longer rooted in these institutions but is spread throughout the social body. As Deleuze phrases it the striated space of disciplinary society is replaced by the

29th September 2012. Vol.5 No.1

ISSN 2304-0777 www.jitbm.com

smooth space of the society of control. Deleuze's sketch-like analysis has been hugely influential for the way postmodern or late capitalist society has been mapped by critical theory. The text has been important for a certain post-structuralist and post-marxist analysis of how power has become ever more decentralized and is now no longer in any straight forward sense connected to easily locatable institutions and exerted by centrally placed actors but is rather spread out in extremely complex structures and networks where it is not possible to excavate the origin or place of power. (Rasmussen) Paul Virilio notes that "the greater is the overall interactivity and the requirement of a panoptic vision and totalitarian world is needed." (Virilio, 1999)

The notion of Panopticon

What is a "Panopticon"? This notion has been extensively discussed by Michel Foucault in his analysis of the prison and disciplinary societies of the nineteenth and twentieth century. Its origin lies in the technical Panopticon, designed by Jeremy Bentham in the late eighteenth century. The description of Foucault based "on the periphery ring buildings in the center, a tower, it is pierced by large windows that open onto the inner side of the ring, the building is divided into peripheral cells, each of which passes through the entire thickness of the building, and have two windows, one inwardly, corresponding to the windows of the tower, and the other to the outside, allowing the light to pass through the cell from side to side. Then simply needs a supervisor in a central tower and to shut up in each cell a madman, a patient, a condemned man, a worker or a schoolboy. Against the effect of light, you can enter the tower, standing out precisely on the light, the small captive silhouettes in the cells of the periphery. Here many cages, so many small theatres, in which each actor is alone, perfectly individualized and constantly visible. The panoptic device landscapes spatial units that can see constantly and to recognize immediately. In short, it reverses the principle of the dungeon, or rather of its three functions - enclose, to deprive of light and to hide - it keeps only the first and eliminates the others. Full light and the eye of a supervisor capture better than darkness, which ultimately protected. The visibility is a trap." (Foucault, 1975)

Visibility is a trap, in the sense that, installing blinds and baffles in the tower, the individual trapped in the cell is seen, but it never sees. Specifically, it is constantly monitored not matter, the point is he knows he can always be, in some way, any "calculation of probabilities" is prohibited. The extreme ingenuity of the Panopticon is this: "induce in the inmate a state of conscious and permanent visibility that assures the automatic functioning of power. Make that surveillance is permanent in its effects, even if it is discontinuous in its action that the perfection of power tends to obviate the news of the year, that this device is a architectural machine to create and sustain a report independent authority of the one who has, in short that prisoners are caught in a situation of power they are themselves the bearers." (Foucault, 1975)

From the panoptic device, this power is invisible, or more precisely, unverifiable, abstract and homogeneous automatic and impersonal. Depersonalized:

29th September 2012. Vol.5 No.1

ISSN 2304-0777 www.jitbm.com

because its effects are independent of the desires that animate the supervisor (curiosity, simple authority, evil). Automatic as "one who is subjected to a field of visibility, and who knows, takes up the constraints of power, he makes them play spontaneously upon himself, he registered himself the power relation in which he plays simultaneously both roles, he becomes the principle of his own subjection." The Panopticon is versatile and adaptable to various institutions and it is the architectural figure of a disciplinary society.

1.2 From the disciplinary society to the control society

The disciplinary society appeared at the end of the 18th century, following the French Revolution, precisely when, new freedoms were proclaimed. To make compatible the republican idea of popular sovereignty (and therefore the power of the anonymous crowd) and the maintenance of public order, ie to find a compromise between efficiency and legitimacy, governments have had to limit and supervise these new freedoms proclaimed. In fact, it has locked people in closed places (hospital, school, factory, prison, family etc…) which allowed continuous monitoring. But according to Deleuze, today's society is a "control society", which is a direct extension of the disciplinary society analyzed by Foucault. Deleuze notes that the various institutions that constitute the disciplinary society is in a state of crisis. The walls of these institutions have collapsed: education tends to become permanent training, home care is widespread, the army humanizes, etc.. In short: you are in the family, but also a bit in the school and already in the business.

The development of technology of control and information has double advantages. The first is to control that is neither apparent nor straightforward. As noted by André Vitalis "in the order of disciplines, the person was asked to intervene to enforce the self-rule, and now in the new economy of surveillance, it is reduced to a mere object information". (Vitalis)

The second benefit is to allow monitoring in a mobile space. According to Deleuze, the disciplinary space gives way to the smooth space of the control society. Structural tunnels of the mole are replaced by endless undulations of the snake. Where the disciplinary society forged castings fixed distinct society control works with flexible and scalable networks. He points out that this society has a global dimension, which is marketing the new form of social control. Indeed, the transition from Fordism to post-Fordist economy (where to go fast, the goal of business is to produce an offer that corresponds exactly to the request) has forced companies to change their strategy and exploit new technologies Computer: increasing the storage and processing of personal data, they are composed of mega-databases to better understand patterns and purchasing behaviour of consumers. Thus a real economy of surveillance releasing large profits has emerged. Illustrated by the example of American Airlines; -this company sold to other companies the services of its booking system, and for 1995, pulled out of profits that more than offset the loss of its transport activities. It is as if most of its activities had increased the physical transport of people and trade processing information-, Deleuze was

29th September 2012. Vol.5 No.1

ISSN 2304-0777 www.jitbm.com

already showing at that time in a somewhat provocative than "marketing form the new breed of masters." (Deleuze, 1990: 177-182)

1.3 Global tele-monitoring system

However, new information and communication technologies have not been used solely or mainly for commercial reasons. In fact, very early, from the outset, states have seen them a new way to more effective control of the population. The context of the Cold War and the current globalization have forced the notion states on the one hand to develop their monitoring systems, on the other hand to cooperate between them. From this point of view, September 11 exacerbated and accelerated the development of a global monitoring system, making both public and legitimate (to fight against international terrorism). In fact this kind of system such as the Echelon network, led by the National Security Agency (NSA) was already existed even before 9/11.

Echelon was born during the Cold War, as a result of an alliance between the United States and the United Kingdom, Canada, Australia and New Zealand, to collect military information about the Soviet Union. The collapse of the communist bloc should be consigned to the activities of the spy network. However, the purpose of the system was shifted: now, it is private and concerned particularly on economic information. Nowadays all worldwide communications (by email, mobile, phone, fax etc…) are routinely intercepted by Echelon, including computers extract mass information messages containing certain keywords.

Another significant example is the creation of the National Imagery and Mapping Agency (NIMA) at the end of 1996. This agency, depending on the Pentagon needed to centralize all views captured by military satellites. It therefore concerned particularly the Security Service Department and Defense. However, since 1997, NIMA aims to control the operation of the flow of commercial imagery in all over the world. As Paul Virilio notes: "After the big ears of the NSA's Echelon network thus open the eyes of the NIMA, illustrating perfectly the statement by the Chief of Staff of the U.S. Air Force in 1997 before the House of Representatives in Washington: "In the first quarter of the 21st century, we will be able to find, track, and target almost in real time any important element moving on the surface of the earth." (Virilio)

These two examples show that it is not an exaggeration to speak of the worldwide tele-monitoring system. Indeed we live in a world where our every action leaves a trace. However, the new information and communication technologies (ICTs) upset top to bottom monitoring devices inherited from the disciplinary society, which were intended to be exercised in an enclosed area. Theoretically, it can cover not only the public space but also the private sphere. Hence, it comes to design absolutely crazy espionage projects, such as Total Information Awareness, developed by the Pentagon under the leadership of General John Poindexter. Ignacio Ramonet explains that this project is to collect an average of 40 pages of information on each of the 6 billion inhabitants of the planet and to entrust their treatment to a hyper-

29th September 2012. Vol.5 No.1

ISSN 2304-0777 www.jitbm.com

computer. By treating all personal data available - card payments, media subscriptions, bank transactions, telephone calls, website visits, emails, police files, folders, insurers, medical information and social security - the Pentagon intends to establish full traceability of each individual." (Ramonet)

2. TECHNICAL AND LEGAL MONITORING DEVICE ON THE INTERNET

2.1. Internet and the "myth" of the network

The term "Internet" is used to designate a set of interconnected networks, and "Internet" all networks using exchange protocols TCP/IP. These protocols have been formally adopted by the U.S. military for their network Arpanet in 1982. It has agreed to distribute free TCP/IP on all existing networks. Originally used primarily by the military and academia, the Internet has "exploded" in the early 1990s, following the creation by the Swiss CERN World Wide Web graphical user interface incorporating text, images, and sounds, thanks to HTML (HyperText Markup Language).

Nowadays, connecting to the Internet has become, for many people a daily act. You can visit a particular website, download programs and files, read messages in "newsgroups", see his personal messaging, chat in real time with people located across the world ... The possibilities of exchange "infinite" Internet provide those that connect to an inevitable sense of freedom. The key feature is the network concept which has nowadays become almost synonymous with Internet. Indeed "the network is at the center of communications technologies. It is the dominant figure. Its scope is largely due to the concept of antiquity and the various uses to which they were made. [...] This tool was hunting, fishing; ornaments - nets and meshes - before designating metaphorically mesh planning nascent and delicate brain connections. Its structure suggests mesh and star connections, and will be used to describe the telephone network and switching, weaving a huge "canvas" enveloping the planet ... We are in contemporary society, with the network as focal image." (Sfez)

This image of the network, rich and suggestive, seems to promise the moon. In fact, it has played an important role in the non-expansion of the Internet itself, but in the discourse that accompanied glorifying speeches, appeared together at the end of the Cold War, heralding the end of the history and the end of ideology. Thus, e-democracy which is emerging will liberate us from barbarism...

Internet is described by his most bitter as both object and subject, responsible for a key brokerage. But Lucien Sfez provides that if an Internet intermediary status is that of an intermediary between generality and universality: "talk to everyone and have access to all the knowledge, the assertions of the Internet, can be understood as a generalization mythically transformed into the universal." The "network" is indeed a myth, in the sense that it is described as a being with its own life (growth, saturation etc...) located "as angels, between the sensible world, and poorly flatly physical and earthly and the sky, air universe, infinite and subtle." (Sfez) But what does the Internet do, concretely the network

29th September 2012. Vol.5 No.1

ISSN 2304-0777 www.jitbm.com

itself do? It grabs the information wherever it is, and stores or exchanges it.

There is no doubt about the ability of the Internet to serve democracy (above all, to serve of freedom and equality between citizens), but also to limit and scope it. Many defenders of network presented Internet as a "global village" where exchanges proliferate and where there is both friendly and anonymity. But "the villages, unlike cities, are they not the place of conformity and mutual monitoring?" (O'Neill)

2.2 Monitoring techniques on the Internet

The recommendations of the National Commission for Informatics and Liberties (CNIL) is clear: "If we stop for a moment to describe Internet" virtual "and other" cyber "to consider it in its real perspective, IT and technical we would find that in terms of anonymity, Internet works like any other place in the world." In fact, anonymity is not the rule on the Internet, and no traces even less. It is possible to be monitored closely if not, at least enough for a market monitoring tools exists and that this monitoring may be the result of very different kinds of players. The CNIL website clearly explains some basic techniques so inexpensive it possible to obtain information about users. CNIL warns that these techniques were not designed to harm users; they each have their justification and usefulness. Among these basic techniques include: environmental variables, cookies, tracing database files to audit the cache. For example, consider the case of the cookie. A cookie is information recorded by the server in a text file on the client computer, the same information server (alone) can go read and edit later. More precisely, a cookie consists of a set of variables (or fields) that the client and server exchange during HTTP transactions, which variables are simply stored on the client in a simple text file. A cookie is necessarily linked to a domain name and a set of URLs so that only one request from the same server can access them. This server has the ability to update or delete a cookie.

Cookies can be used for many different purposes. As a concrete example: a customer, for any reason, leaves his contact information on a website. On this occasion, the server of this site can deposit in the client computer a cookie containing the coordinates. Nothing prevents thereafter, to the link between the client's IP address, and mailing address to be aware so that registered the course followed.

In general, cookies are not used for purposes of monitoring unhealthy, but most often for commercial reasons (dynamic display banners personalized pages created dynamically based on the profile etc…). The problem is that it is difficult, if not impossible, to distinguish between servers that use cookies to improve the comfort of the consultation, and those who hunts and observes client unwittingly using the same means.

Should we be afraid of all the cookies? This technique can certainly produce an impression of manipulation, but be aware that a cookie cannot contain much or have any particular action. This surveillance technique, like others, they present a character need technical (environment variables, file audit) is not in

29th September 2012. Vol.5 No.1

ISSN 2304-0777 www.jitbm.com

itself particularly harmful. But it is the processing and duplication of information obtained in very different ways, which can sometimes be a real violation of the right to privacy and confidentiality of personal privacy.

In fact, the concern related to abuse control techniques is not new. To prevent the most obvious draconian dangers some laws on the protection of personal data emerged since the 1970s. With the advent of the Internet has been a real legal arsenal to protect online privacy: the right to use anonymous means of payment and encryption techniques, the right not to reveal his calling number in advanced telephone networks, the right to use anonymous access means, etc.. More generally: the right to prior information, right to oblivion, right of access, right of opposition ... The problem is that on the one hand, Internet users in general do not know their rights, and other hand, technological progress and more rapid legal regulation makes very delicate.

2.3. Legal measures taken in the USA since 9/11

The events of September 11 have changed the government's attitude towards human rights and personnel life. The priority given to the fight against terrorism and cybercrime tends to shatter the legal constituted for years in order to protect citizens against threats to their freedom. Thus, the non-governmental organization Reporters Without Borders (RSF) notes that "if the United States is at the origin of the Internet, they are also the first to have implemented the tools of monitoring technology of communication. The September 11 attacks have only strengthened the willingness of the authorities to control the flow of information on the Web." (RSF, 2003) Indeed, the supposed terrorists use the Internet to prepare attacks led the U.S. government to take a series of measures to increase flexibility and opportunities for online monitoring. Here is a short simple list of these measures about the change of government approach vis-à-vis the network.

From September 13, 2001, the law "Combating Terrorism Act" allows American security services use software Carnivore wiretapping without the consent of the court. Specifically, the FBI may order electronic monitoring of a person for 48 hours without having to seek the approval of a judge.

October 24, 2001, the adoption of the text "Provide Appropriate Tools Required to Intercept and Obstruct Terrorism" finally legalized the use of Carnivore. For this, the FBI will only need the endorsement of a special court whose activities are confidential.

The "Homeland Security Act" (HSA) of 20 November 2002 allow service providers to reveal a local or federal content of electronic communications. Thus, the law establishes a transfer of responsibilities: the supplier assumes the role of a judge. In addition, some organizations defending civil liberties have complained that these revelations on the basis of "good faith" and not that of a "reasonable belief" and thus expressing a concern about the risk of one widespread denunciation. "The 484-page Act prescribed the biggest change in the federal government in over 50 years. Its passage,

29th September 2012. Vol.5 No.1

ISSN 2304-0777 www.jitbm.com

on November 25, 2002, consolidated more than 20 existing federal agencies into a single Homeland Security Department, including the Federal Emergency Management Agency (FEMA), the U.S. Secret Service, the U.S. Customs Service, the U.S. Coast Guard and the Immigration and Naturalization Service (INS). Not since President Truman created the Department of Defense in 1947 has the federal government undergone such dramatic restructuring. The purported aim of this consolidation was to detect and eliminate emerging terrorist threats by removing information firewalls between government agencies, and centralizing the unprecedented flood of surveillance data made possible by the USA PATRIOT Act. However, civil liberties groups have objected strongly to the Homeland Security Act from the start, contending that it is characterized by three disturbing trends: reduced privacy, increased government secrecy and power and strengthened government protection of special interests. Allen Weinstein, president of the Center for Democracy in Washington, DC, has called it a "law of unintended consequences." (9-11 Research)

Another important point is the cryptography. The cryptography is a method for Internet users, with encryption software to protect the confidentiality of information exchanged on the Internet. Cryptography has never been banned in the United States. However, since September 13, Senator Judd Gregg offers a comprehensive ban on cryptographic software (specifically, those broadcasters would not have provided the public authority the decryption key). Certainly, terrorist networks use certainly encryption software, but the creator of Pretty Good Privacy software (PGP), David Zimmerman, recalls that "together, we discussed this issue during the last decade. And together, we decided that the company had more to gain than to lose from strong cryptography. It must not be forgotten that cryptography saves lives worldwide. The PGP is used by organizations defending human rights around the world, especially under dictatorships." (RSF, 2003)

Finally, the Total Information Awareness project mentioned above is the culmination of this package that RSF describes it "draconian." "The post-9/11 world is now clearly drawn... Destabilised and on the defensive, the leading democracies are gradually eroding the space for freedoms. The economically most powerful dictatorships arrogantly proclaim their authoritarianism, exploiting the international community's divisions and the ravages of the wars carried out in the name of the fight against terrorism. Religious and political taboos are taking greater hold by the year in countries that used to be advancing down the road of freedom."(RSF, 2008)

2.4 In Europe

Since 9/11, globalization is certainly still a globalization of trade and financial flows. But it has also become the global fight against terrorism, and therefore requires increased cooperation between states in security. In this context, the measures mentioned above are not only the U.S. but all countries of the world. Included the European Union (EU).

Some European countries have passed Law on Everyday Security (LSQ).

29th September 2012. Vol.5 No.1

ISSN 2304-0777 www.jitbm.com

Among other measures, these acts for example:

- Obliges to one year shelf archives of all online activities of customers and data sending and receiving e-mails by providers of Internet access.

- Allows judges to resort to "means the State subject to secret national defense" to decrypt the messages. It thus obliges providers cryptographic means to provide authorities with their encryption protocols (from this point of view, France for example is ahead of the United States).

After 9/11 the European institutions largely revised their previous position, which was against to any form of "electronic surveillance widespread or large-scale exploratory." Thus, The European Parliament Civil Liberties Committee approved in July 2001 a report by Italian MEP Marco Cappato: This report strictly framed the right of access to police files to audit suppliers Internet access (as well as telephone companies). To be able practice such authorization: "Member States of the Union shall act under a specific law which is comprehensible to the general public and their actions must be quite exceptional, authorized by judicial or competent in specific cases and for a limited duration, appropriate, proportionate and necessary in nature related to the democratic society."(RSF, 2003)

However, since the attacks, the U.S. position, for example supports the principle of conservation of automatic data connection, opposes the principles outlined in the report. On 30 May 2002, under pressure from the Council of Europe, MEPs adopted a new directive aimed at introducing common rules on data retention.

Moreover, the first international convention against cybercrime was signed on 26 November 2001 in Budapest. It is the first ever international treaty on criminal offences committed against or with the help of computer networks such as the Internet. This text, organizes:

- The supply of information or computer storage media that contain private information relevant to the security services in the course of their investigations.

- The supply of information stored in the providers and services.

- The search sites and servers and they extend these searches to computer networks.

- The preservation and storage of data input.

- The real-time collection of information and logs connections if needed (the judicial authorities may require that these operations are performed by providers and services).

The NGOs do not deny the usefulness of being able to identify a subscriber to trace the source of a crime. But this does not justify such widespread and exploratory measures affecting all citizens. Technically, only targeted interventions appear feasible. The head of the AFA (French Association of Service Providers and Internet Services) Jean-Christophe Le Toquin said: "Keeping the trace of all the exchanged emails is a utopia, even if we keep not the content of the messages, except that the focus is no

29th September 2012. Vol.5 No.1

ISSN 2304-0777 www.jitbm.com

longer the political development of the information society, but his blasting.... To keep an ocean of data, you need the tools of exploitation and police technicians go with it." Professionals and Internet operators are currently in limbo.

3. DEMOCRACY AFTER 9/11

Since eleven years, we live in the memory and the consequences of 9/11. Beyond the geopolitical reorganization triggered by the 9/11, it is our vision of democracy, freedom and security that have been called into question. Widespread surveillance of civilian populations is in progress. We use terrorism to scare and to restrict fundamental freedoms. The reduction of civil liberties in the name of security is still going. You go to the USA with a computer and your mobile phone. Under current law, the U.S. services you are entitled to seize, emptying their contents, to transfer their material to them, then you make your business or not. That's all. But I wonder if indeed this application is part of a real fight against terrorism. (Léchot)

Thus, the 9/11 events "surely changed the global political landscape forever. The shockwaves it sent throughout the world, most notably through the United States, raised hopes that the tragedy would encourage probing of the causes of the event and help change Western governments' foreign and military policies and adventures in the interest of reducing global tensions. That has hardly happened. If anything, the wars in Afghanistan and Iraq and more recently Libya have escalated tensions, conflicts, and lawlessness in parts of that region. The policies of the so-called war on terror, the extensive buildup of intelligence and surveillance apparatuses and security measures in the United States, Canada, the United Kingdom, and other Western countries, have also proved tension-inducing. Racial profiling, severe restrictions on the liberties of ordinary citizens, and the widespread interrogation and detention of individuals of Middle Eastern and North African origin have harmed a sense of belonging and instigated destructive radicalism among youth of Muslim origin. All these have opened an ever-deepening psychological, emotional, and increasingly, cognitive gulf between Western and Muslim-majority nations and by extension between citizens of European ancestry and diasporas of Muslim origin in the West. This is one of the most tragic and perhaps lasting calamities caused by 9/11, as a live-and-let-live attitude that prevailed among citizens in these societies has now been replaced by a mutual sense of resentment and distrust, fear, anxiety, and psychological insecurity. The celebrated national narratives of Western democracies about human rights, the rule of law, equality before the law, civil liberties, and democratic rights have also been discredited and mocked. The climate of fear and more fear on the part of the larger society and the out-of-proportion reactions by Muslim populations have made life more insecure than ever before. Hence, from country to country, security-driven immigration and settlement policies focus on how to watch, contain, and control Muslims and thus protect their societies from cultural contamination. (Moghissi)

Some analysts have realized that the term of democracy is insufficient to describe the way of operation of our

29th September 2012. Vol.5 No.1

ISSN 2304-0777 www.jitbm.com

societies and, it is necessary to add a term to describe the violence of the system or ignore the idea of democracy. For example Claude Lefort talks about a "new democratic society" that he calls it "the wild democracy" (démocratie sauvage). (Lefort, 1981:29) Gilles Châtelet brought up the idea of markets democracy (démocratie-marché)**.** (Châtelet, 1998:142)

Conclusion

We have tried to show how the Internet crystallizes all the ethical and technical problems related to monitoring democracy. We have seen that these problems are, in the context of post-9/11, greatly exacerbated. In fact, if in the previous period (the fall of the wall 9/11's wall), the watchword of the Western powers was to spread democracy, praising and propagating its virtues today, it is more spread, but to safeguard democracy (although sometimes this backup may take the form of "save as spreading"). To achieve this goal, the policies of the Western powers are carried out under an imperative and invariable: living in a safer world and fighting against the terrorism.

New surveillance technologies already offer powerful means to counter the actions of terrorist and criminal networks. The shock of the September 11 attacks, led the U.S. and European governments to enact laws aimed at increasing flexibility and the use of these controls. But by giving the technical and legal possibilities to monitor to prevent the actions of a few, these governments rely heavily involved some liberties (under, essentially, the right to confidentiality and privacy). This leads to a paradoxical situation: to save democracy that we are ready to repudiate some of its fundamental principles. In short: to save democracy, it is put in danger, the danger from the collapse of boundaries between public space and private space, which may occur with the use of massive, widespread and uncontrolled network station.

These are not the techniques themselves that are to blame, but the use made of it. In this regard, the CNIL recommends responsible use of computer technology by informing rights, respecting the laws, denouncing illegal activities, but also and especially by participating in a complex debate whose stake is the future democracy. All these technical capabilities, combined with the legal means to monitor everyone all the time are they evidences of a totalitarian democracy?

REFERENCES

André Vitalis, Informatiques et libertés : une problématique toujours pertinente, disponible à l'adresse http://cazes.cnam.fr/QNPI/Actes/InformatiqueLiberte.html.

Bernard Léchot, "2001-2011, les libertés bradées", http://www.swissinfo.ch/fre/politique_suisse/20012011,_les_libertes_bradees.html?cid=30995736.

Claude Lefort, L'invention démocratique, Fayard, 1981.

CNIL (Commission Nationale de l'Informatique et des Libertés), http://www.cnil.fr.

Gilles Châtelet, Vivre et penser comme des porcs. De l'incitation à l'envie et à l'ennui dans les démocraties-marchés, Exils, 1998.

29th September 2012. Vol.5 No.1

ISSN 2304-0777 www.jitbm.com

Gilles Deleuze, 1995, Control and Becoming, (trans), Martin Joughin, Negotiations, New York, Colombia University Press, pp.177-182.

Gilles Deleuze, "Post-scriptum sur les sociétés de contrôle" in Pourparlers", Editions de Minuit, 1990.

Haideh Moghissi, "What We Have Learned from 9/11", http://essays.ssrc.org/10yearsafter911/what-we-have-learned-from-911/

Ignacio Ramonet, "Surveillance totale", Le Monde Diplomatique, août 2003.

Ignacio Ramonet, "Adieu libertés", Le Monde Diplomatique, janvier 2003.

Lucien Sfez, "Internet et les ambassadeurs de la communication", Le Monde Diplomatique, mars 1999.

Michel Foucault, "Surveiller et punir", Gallimard, 1975.

Mikkel Bolt Rasmussen, "The Control Society After 9/11", http://darc.imv.au.dk/publicinterfaces/wp-content/uploads/2011/01/Bolt.pdf.

Mathieu O'Neill, "Internet, ou la fin de la vie privée", Le Monde Diplomatique, septembre 1998.

Philippe Rivière, " "Grandes oreilles" américaines", Le Monde Diplomatique, mars 1999.

Paul Virilio, "Le règne de la délation optique", Le Monde Diplomatique, août 1998.

Paul Virilio, "Télésurveillance globale", Le Monde Diplomatique, août 1999.

RSF, "Internet sous surveillance", Rapport Internet 2003 disponible à l'adresse http://www.rsf.org/rubrique.php3?id_rubrique=377.

RSF, "Only peace protects freedoms in post-9/11 world", Press Freedom Index 2008, http://en.rsf.org/press-freedom-index-2008,33.html.

William Bloss, "Escalating U.S. Police Surveillance after 9/11: an Examination of Causes and Effects", http://www.surveillance-and-society.org/articles4(3)/escalating.pdf

9-11 Research, "The Homeland Security Act, Legislation Predicated on the Official Story of the 9/11/01 Attack", http://911research.wtc7.net/post911/legislation/hsa.html