University of Alberta

Is it Possible to Regulate the Internet Globally?: a Comparative Case Study of the Cybercrime Framework in Canada and Romania.

by

Dan S. Manolescu

A thesis submitted to the Faculty of Graduate Studies and Research
in partial fulfilment of the requirements for the degree of

Master of Arts

in

Humanities Computing

Fall 2009

Edmonton, Alberta

Examining Committee

Dr. Stan Ruecker, Humanities Computing

Dr. Geoffrey Martin Rockwell, Humanities Computing

Dr. Sean Gouglas, Humanities Computing

Abstract

In this thesis, I investigate the concept of Internet regulation and its implementation by examining the Convention on Cybercrime, which regulates the European Union (EU) and non EU countries. I examine the approaches taken toward the Convention on Cybercrime in two different socio-economic and political systems: Canada, a modern democracy that only signed the Convention, and Romania, an ex-communist democracy that both signed and ratified it. With this Convention, the Council of Europe has claimed that one model of global Internet regulation is appropriate for all countries. I argue that the infrastructure and legal, economic, and socio-cultural aspects of local cultures make the global homogenous regulation of the Internet impractical, therefore regulation on a national level would be more effective. I also try to contribute to current research by studying the complexity of the global regulation of Internet crimes by demonstrating: the importance of democracy and technology for public policy frameworks for cybercrime, by describing; the limitations of the model represented by the global monolithic Convention on Cybercrime, and by suggesting that a universal democratic model of global Internet regulation is utopian and does not address the individual needs of each country.

Acknowledgements:

I would like to thank to my family, especially to my grandparents, mamaia, buni, tanti Janeta, and mosu, and my parents, Doina and Tata, for their support in getting my education.

Thank you!

“non scholae sed vitae discimus”

We learn not for school, but for life.

Table of contents

Abstract.....I

Acknowledgements.....II

Introduction.....1

Chapter One: Theoretical Issues concerning the Convention on Cybercrime Framework..... 5

Chapter Two: Canadian Cybercrime and its Regulation.....21

Chapter Three: Romanian Cybercrime and its Regulation.....34

Chapter Four: Regional Adoption of International Conventions…….…….....45

Conclusion.....57

Bibliography.....65

Appendix 1……72

Appendix 2……73

Table 1……...91

Introduction

In 1974, the first search network between academic and research sites, based on the ARPANET project,[1] came into being. Thirty years later, in 2004, the Council of Europe implemented the Convention on Cybercrime, the first international treaty devoted to Internet-related crimes. The Council of Europe found the Convention was needed because technology and law are connected today on a global level. This thesis addresses the contemporary issue of cybercrime, questioning the relationships among democracy, developing Internet technology, and cyber-space-related crimes all over the world.

My scholarly interest in the field of cybercrime started in 2007 when, on the one hand, more and more information about computer-related crimes within the ex-communist Eastern European countries became the subject of public discussion, and, on the other hand, cybercrime legislation within North America and European countries became the subject of international debate. This discussion raised my interest in the regulation of cybercrime within the global village. I asked the following question: is global Internet regulation needed within the newly emerging Internet crime domain, and what does "cybercrime" mean in relation to traditional crime? If such regulation is necessary, can global Internet regulation (i.e., cyber-law) adjust to specific regional cultures? How do different democracies, cultures, social organizations, and economic policies contribute to global Internet regulation?

---

[1]The ARPANET was developed in the 1960s as a network project of the U.S. Department of Defence's Advanced Research Projects Agency. For a detailed history of the building of the ARPA network and Internet, see Janet Abbate, "From ARPANET to Internet," *Inventing the Internet* (Cambridge: MIT Press, 1999) 113-146.

In this thesis, I will consider the notion of Internet regulation, focusing on the cyberspace regulation called the European Convention on Cybercrime,[2] which is a state public regulation issued on 23 November 2001 to regulate European Union (EU) and non-EU countries. This Convention on Cybercrime was only signed by Canada, a modern democracy, but was both signed and ratified by Romania, an ex-communist democracy[3].

My first objective is to discuss the Convention on Cybercrime, which is the current theoretical framework for responding to cybercrimes (e.g., credit/debit card electronic fraud, identity theft, child pornography) and to contribute to current Internet legislation research by asking relevant questions about the global contemporary Convention on Cybercrime. My second objective is to compare the implementation of the above cybercrime framework in two democracies (the Canadian historically established democracy and the ex-communist Romania with its newly emerging democracy). Both states have signed the European Convention on Cybercrime, but only Romania has ratified it. What have been the results? Is the Romanian technological infrastructure capable of being effective? Why did Canada not ratify the Convention on Cybercrime? Was the infrastructure the problem or was it the federal and provincial governments' intricate network of legislation? Was the problem the right to privacy or

---

[2] Council of Europe. Convention on Cybercrime ETS no 185, 23 November 2001. 3 Jan 2009 <http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=185&CM=8&DF=9/5/2007&CL=ENG>.

[3] Canada signed the Convention on Cybercrime on 23 November 2001. Romania also signed it also on 23 November 2001 and ratified it on 12 May 2004. The Convention entered into effect on 1 September 2004. For more details about the total number of states that signed and/or ratified it as of 15 May 2007, see Alexander Seger, "The Convention on Cybercrime of the Council of Europe." 2nd WSIS Action Line C5, Geneva, 14-15 May 2007. 20 Jan. 2009 <www.coe.int/economiccrime> or the website of the Council of Europe http://conventions.coe.int

the Convention's questionable global usefulness? Where is the boundary between government self-regulation and government coercion?

Specifically, I question the Council of Europe's claim that one form of global Internet regulation is appropriate for all countries. I argue instead that the infrastructure, legal, economic, and socio-cultural aspects of local cultures affect the global homogenous regulation of the Internet. The relationship between the global model of Internet regulation (i.e., the Convention on Cybercrime) and its individual implementation in specific countries and legal frameworks (e.g., legislation concerning consumer privacy or human rights) is problematic. Still, cybercrime is a global issue due to its technological features (i.e., its borderless nature and trans-national impact). In particular, I look at Canada's and Romania's infrastructure, legal, economic, and socio-cultural differences (e.g., human behaviour, public morality, level of national corruption, self-regulation), which affect the implementation of an international treaty like the Convention.

This thesis has four chapters and a conclusion. In Chapter One I investigate the conceptual and historical context of the Convention on Cybercrime. I examine its content, terminology, and define "cybercrime" and "Internet regulation" and its features that inform contemporary public and private spaces. I also look at how the Convention is recognized locally and globally, and what a convention or treaty related to Internet regulation is. In Chapter Two I provide data about the Canadian democracy in relation to technology and economic power which questions Canada's action regarding the Convention on Cybercrime. I use cybercrime statistics to examine why Canada, a democratic multicultural state with a liberal ideology and welfare state policy, has signed but not ratified the Convention on Cybercrime. In Chapter Three I provide data about Romania in relation to its democracy, technology and economy, which provokes questions as to why and how the Convention on Cybercrime was implemented. In the context of Romania's

recent democratic practice, I will examine why Romania – with a weak democracy and economy -- as opposed to Canada, has signed and ratified the Convention on Cybercrime.

In Chapter Four I compare the regional adaptation of international conventions on cybercrime in Canada and Romania. The relationships among democracy, technology and privacy are important and are questioned while considering cybercrime statistics, human rights, demographics and corruption issues in both countries. The conclusion will summarize the four chapters, and, based on the examples of Canada and Romania, argue that the Convention on Cybercrime is not suitable to effectively fight against Cybercrime due to national differences in legal infrastructure, as well as economic and socio-cultural differences.

The research for this thesis included primary and secondary sources in English as well as in Romanian (my native language). My methodology involves an interdisciplinary approach making use of political, technological and socio-cultural histories. I collected data and produced a bibliography in progress during my library research, which included the use of inter-library loans, and consulted a number of important foreign sources in their original locations. I also made use of historiography to contribute to the study of Internet crimes by discussing a controversial contemporary model of global Internet regulation: the Convention on Cybercrime.

Chapter One: Theoretical Issues concerning the Convention on Cybercrime Framework

"Cybercrime: a Threat to Democracy, Human Rights and the Rule of Law" is the opening title of the Council of Europe's webpage dedicated to this issue.[4] In this section, I study the notion of "cybercrime," the rationale and the evolution of the Convention on Cybercrime and their acknowledged significance, trying to understand why and how the Convention was developed. Since the Internet operates globally, the cybercrime law framework also needs to operate globally, but faces difficulties in doing so. Computer-related crimes are borderless but the law is limited nationally while still nonetheless trying to operate globally under the recommendations of the Convention on Cybercrime. The issue to be addressed is the definition of "cybercrime" and how it is recognized locally and globally, and describing what a convention or treaty related to Internet regulation is. Moreover, this cybercrime convention employs a specific apparatus and actors that never existed before (i.e., Internet victims, cyber offenders, and new media for cyber police). Thus, the practice of traditional law is encountering new situations due to the nature of cyberspace.

I will examine the historical roots and debates regarding the content and aims of the Convention on Cybercrime, which was drafted by the EU and signed and ratified by the EU and some non-EU countries. Then I will look at the meaning and rationale of this convention in relation to the notion of "treaty" within a global world and what it implies. The features of Internet regulation will also be summarized.[5]

---

[4] Council of Europe. 4 April 2009 <http://www.coe.int/t/dc/files/themes/cybercrime/default_en.asp>.

[5] For a synthetic diagram showing the actors involved within the Internet regulatory framework, see Hwa Ang Peng, How Countries Are Regulating the Internet Content. 20 Jan. 2009 <http://www.isoc.org/inet97/proceedings/B1/B1_3.HTM#s11>.

The content and computer-crime terminology used in the Convention on Cybercrime will be looked at to identify the features of cybercrime. Also, the main elements involved in cybercrime will be studied (i.e., the typology of crimes, the offenders, the use of the computer as a tool, the Internet as a medium, and legal activities). The notions of "international cooperation," "public"and"private space" will be examined.

The Internet has been described as "a new media" developed in the United States by the Department of Defence's Advanced Research Projects Agency (ARPA) and then by American universities.[6] In its simplest form, the Internet is a connection or network (through telecommunication cables or wireless links) of different computers all over the world. The Internet originated in the 1960s, but Internet offences and cyber offenders did not become common until the late 1990s, when the rapid pace and spread of technology development made such offenses a common occurrence. By 1996, the U.S. government's ownership of the Internet network ended and the transition from governmental public to private (academic, commercial, non-profit) use of the Internet began.[7] During this period, significant numbers of new media offences and cybercrime offenders started to emerge.

In 2001, the Council of Europe raised the issue of pervasive Internet criminal behaviour and made a strong argument in favour of cybercrime regulation. According to the Council of

---

[6] At the beginning, in the 1960s, ARPAnet consisted of four server computers. Finally, by 1971, the University of California at Berkley developed the Transmission Control Protocol/ Internet Protocol (TCP/LP), which helped one computer to read and process data coming from another computer. For more details on Internet history, structure and function see Natascha Gerlach, "The New Media Described," "Regulating the Internet: A Futile Effort? The Case of Privacy in a German-Canadian Comparative Study," L.L.M. thesis Queen's University at Kingston, 1999, 3-11. For a fascinating discussion of military technology, "packet switching" technology, economic models and the origins of the Internet, see Janet Abbate, "Government, Business and the Making of the Internet," *Business History Review* 75.1 (2001): 147-176.

[7] Abbate, *Government* 171-176.

Europe's explanatory report on the Convention on Cybercrime, "Information technology has in one way or the other pervaded almost every aspect of human activities."[8] The previous communication technology (telephone, radio, TV, and film) has been increasingly replaced by a new medium for exchanging information: computers and the Internet. The Internet has resulted in positive changes to our social habits and cultural norms. However, the democratic phenomenon of mass accessibility to personal and commercial information and electronic mail has been paralleled by prolific criminal activity, including new types of crimes. In 2001, the Council of Europe noted that

> the consequences of criminal behavior can be more far-reaching than before because they are not restricted by geographical limitations or national boundaries…. The new technologies challenge existing legal concepts. Information and communications flow more easily around the world. Borders are no longer boundaries to this flow. Criminals are increasingly located in places other than where their acts produce their effects.[9]

A blurring of national and international (trans-national) space for Internet regulation has occurred. The Council of Europe made a solid argument for subjecting the new sophisticated technologies to criminal law which laid the foundation for the global Convention on Cybercrime for EU and non-EU states. This convention which regulates the Internet globally, is a state public regulation issued on 23 November 2001 and came into effect on 1 September 2004; according to the world map of the implementation of the Convention on Cybercrime, as of March 2009 (Appendix 1), it had been ratified by 23 countries (including the United States) and signed by 22 countries (including South Africa, Canada and Japan).[10]

---

[8] Council of Europe. *Convention on Cybercrime: Explanatory Report. ETS no 185*, 14 November 2001. 3 Jan. 2009 <http://conventions.coe.int>.

[9] Council of Europe, *Convention on Cybercrime: Explanatory Report.*

[10] According to the world map on the implementation of the Convention, "over

This convention is the first international treaty aimed at global Internet regulation. This treaty has the effect of a convention as an international agreement among states[11] and is to be applied worldwide, but needs, if possible, to be ratified and implemented in each country. The Convention on Cybercrime has to keep up with the pace of social and technological change. Because of the increase in criminal activity and the rapid development of society, the Convention on Cybercrime received an additional Protocol on racism and xenophobia that came into force on March 1, 2006.[12] Also, the contemporary issue of cyber-terrorism is of increasing importance.

The Convention on Cybercrime has four major chapters dedicated to defining its terms (i.e., cybercrime), the measures to be taken at the national level (e.g., procedural law, jurisdiction), international co-operation (including the principles referring to co-operation, extradition and mutual assistance), and final provisions (signing the Convention and its

---

100 countries worldwide are now reinforcing their legislation, taking inspiration from the Convention as a guideline or a <model law>". This map was made public on the occasion of the conference **"**Criminalising Child Pornography, Training, Tracking Money on the Internet: Programme Features of the 2009 Council of Europe Conference on Cybercrime" hold in Strasbourg on 9-10 March 2009. 2 April 2009. https://wcd.coe.int/ViewDoc.jsp?id=1414219&Site=DC&BackColorInternet=F5CA75&BackColorIntranet=F5CA75&BackColorLogged=A9BACE. In order to compare the pace of signing and ratification (authorized approval) of the Convention on Cybercrime, see more details in Seger about the total number of states that signed and/or ratified it as of 15 May 2007.

[11] For more details about treaties research, terminology and history see the American Society of International Law, *ASIL Guide to Electronic Resources for International Law*, 5 April 2009 < http://www.asil.org/treaty1.cfm>. For an extensive glossary on European Union treaties see European Commission, *Treaties Office Database*, 5 April 2009 < http://ec.europa.eu/world/agreements/glossary/glossary.jsp?internal=true>.

[12] For more details, see Council of Europe. *Additional Protocol to the Convention on cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems CETS No.: 189*, 27 March 2009 < http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=189&CM=8&DF=17/02/2006&CL=ENG>. Canada and South Africa where the only non-EU countries that had signed this protocol as of 5 April 2009.

implementation, accession, ratification, and so on). The Convention recommends that this guideline be followed in all cases: "Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the access to the whole or any part of a computer system without right."[13]

The Convention on Cybercrime defines the specific terminology related to the crimes committed via the Internet and other computer networks (i.e., network, computer system, computer data, service provider and traffic data, and cyberspace offences with trans-border character). For example, the Convention explains how cyberspace is created: "by connecting to communication and information service, users create a kind of common space … which is used for legitimate purposes but may also be the subject of misuse."[14]

The terminology addressing computer-related crimes refers to different levels: the level of the confidentiality, integrity and availability of computer data and systems (involving, for example, illegal access, illegal interception, data interference, system interference, misuse of devices); the level of computer-related offences (e.g., computer-related forgery and computer-related fraud); the level of content-related offences (e.g., offences related to child pornography); and the level of offences related to infringements of copyright and related rights.

The government is one of the contemporary actors involved within the Internet regulatory framework. According to Hwa Ang Peng, a contemporary theorist on Internet crime who works at the Singapore Internet Research Center, when discussing the five steps of Internet supervision, specific actors are involved in cyber regulation, ranging from the government policy makers to

---

[13] Council of Europe, *Convention on Cybercrime.*

[14] Council of Europe, *Convention on Cybercrime: Explanatory Report.*

the government regulators (Table 1).[15] The mechanism of regulation ranges from self-regulation with self-sanction to legal regulation with state enforcement and coercive sanctions. Peng argues that Western and non-Western countries differ in terms of the tradition of free speech and free press, concluding that "any common areas of regulation, for example in racial and religious speech, will be applicable only in culturally similar areas." Germany, for instance, is concerned with anti-Semitic speech, but this concern is not as widely shared as is the concern with child pornography.[16] Moreover, Peng states that "the European Union's code of ethics for the Internet is unlikely to be satisfactory to all. Either the code will have very broad principles or else another layer of national code will be needed by each European country. "[17] Existing technology is also important when regulating the Internet and it seems that "each regulator, therefore, has to consider the country's framework and regulate the Internet to its own perceived needs and benefits."[18]

The concepts of "cybercrime"[19] and "Internet regulation"[20] related to the "global information society"[21] (GIS) refer to crimes committed all over the world by using computers

---

[15] For an essential analysis of the approaches adopted by countries (United States, France, China, Singapore) that have attempted to regulate Internet content see Hwa Ang Peng, "How Countries Are Regulating the Internet Content," 20 Jan. 2009 <http://www.isoc.org/inet97/proceedings/B1/B1_3.HTM#s11>.

[16] Peng "How Countries."

[17] Peng "How Countries."

[18] Peng "How Countries."

[19] For the relationship between cybercrime and cyberspace, see Sara M. Smyth, "Child Pornography on the Internet: An International "Crisis" from a Canadian Perspective," diss., York University, 2008, 148-160.

and Internet connections. The notion of global Internet regulation has been studied by scholars[22] who have indicated its theoretical limitations. The notion of regulation can be understood generally as "the imposition of standards and legally enforceable controls,"[23] which is done by a body of state institutions (i.e., the government) in order to officially control individuals and private entities.

One of the weak and uncontrollable features of government Internet regulation is linked to the human factor. As Julian Ding has stated:

> The rules and laws that govern human behavior have traditionally been limited by the geographical boundaries of the state. With the Internet, these geographical boundaries, to a great extent, have disappeared. Accordingly, there is uncertainty as to how to regulate the Internet. It is necessary to distinguish between rules affecting the Internet and rules affecting the activity which requires the use of the Internet.[24]

---

[20] For a theoretical approach to the concept of "Internet regulation," see Julian Ding, "Internet Regulation," *Legal Issues in the Global Information Society,* eds. Dennis Campbell and Chrysta Ban (New York: Oceana Publications, 2005) 279-351.

[21] For a complex analysis see Christopher Marsden, ed., *Regulating the Global Information Society,*Warwick Studies in Globalisation (London; New York: Routledge, 2000).

[22] For a discussion of the tension between Internet regulation and the right to privacy, see Eve M. Caudill and Patrick E. Murphy, "Consumer Online Privacy: Legal and Ethical Issues." *Journal of Public Policy & Marketing* 19.1 (2000): 7-19.

[23] For an explanation of the characteristics of regulation and the theoretical perspectives for government regulation (market failure, public interest, life cycle and private interest), see Ding 281.

[24] Ding 287. For more details on Internet law and cyberspace regulation, see Lawrence Lessig, *Code and Other Laws of Cyberspace* (New York: Basic Books, 1999); for more information on cyber-regulatory environment and cyber lawyers, see Andrew Murray, *The Regulation of Cyberspace: Control in the Online Environment* (Abingdon: Routledge-Cavendish, 2007).

Regulation of the private neo-liberal US market is needed in terms of the urban hierarchy within the same national state.[25] This concept of hierarchy can be extended to the notion of a global technological and economic hierarchy which has impacted Internet development, cybercrime and the implementation of the Convention on Cybercrime.

In order to define cybercrime in relation to cyberspace, some researchers use the "cyberspace as place" metaphor.[26] According to this idea, cyberspace is a unique democratic virtual environment for a utopian society where the control begins bottom-up. The problem within this metaphorical space is how and why an entity (i.e., a democratic or a dictatorial state and its government) would apply legal regulations in cases of cyber offences. This problem raises a paradoxical issue of the legitimacy of a superior body with social and physical limitations within a democratic virtual structure. Cybercrime is borderless and transnational due to the Internet's features (its democratic spread and access all over the world, which is highly connected with the technological development of local communities and national states).

A law regarding Internet crimes is needed, but the connection between the development of technology and that of society is problematic. Cybercrime legislation is experimental because the rule-making process is still in progress and is trying to parallel the development of the Internet.[27] Thus, cybercrime legislation is a dynamic body of rules and its apparatuses (cyber-police and cyber-lawyers).

---

[25] Edward Malecki, "The Economic Geography of the Internet's Infrastructure," *Economic Geography* 78.4 (2002): 399-424.

[26] Smyth 148-166.

[27] Hwa Ang Peng, *Ordering Chaos: Regulating the Internet* (Singapore: Thomson Learning, 2005) 175.

Cybercrime and cyber-law involve private (users) and public actors, so Internet-related crimes and legislation raise problematic issues such as privacy rights versus the greater public good. In this context, private and public space blend together. For example, in the United States, a controversial debate is occurring on transposing the Convention on Cybercrime recommendations into domestic federal law. Moreover, a common legal framework for the enforcement of borderless cybercrime is necessary, but in the United States, legislators must consider First Amendment free speech principles. Given these conditions, it seems likely that a common legal framework for fighting cybercrime globally may not be possible. Previous research concluded that user privacy involves unresolved issues such as the ownership of consumer information.[28] There are concerns regarding disruptive technology and privacy-destroying technologies because of the importance of privacy for the non-offending Internet users.[29] In some situations in terms of the neo-liberal policy, economic rights take precedent over democratic rights, and thus the "public interest" is of less importance.[30]

In this case, self-regulation has been suggested as an alternative to governmental regulation of the Internet. Some scholars have advocated for user responsibility and self-regulation to prevent cybercrime, but self-regulation seems to be ineffective and utopian and is unlikely to be the best option for limiting Internet crime.[31, 32] It is not the best option because

---

[28] Caudill and Murphy 13.

[29] Michael Froomkin, "The Death of Privacy?," *Stanford Law Review* 52.5 (2000): 1461-1543.

[30] Andrew James Reddick, " The Duality of the Public Interest: Networks, Policy and People," Diss. Carleton University, 2002.

[31] Lisa Dawn Clyburn," Internet Crimes: Can and Should the Internet be Regulated?," M.Ed. thesis University of Alberta, 1998.

each individual's concept of right or wrong in terms of ethics and morals differ. Therefore, what is right for one person might not be right for a different person. For this reason, self-regulation is not an effective option for regulating the Internet at a global level.

Thus, the Convention on Cybercrime as a "canonical" global model for Internet regulation is problematic and raises some issues related to technological development, the non-Western world, censorship (in China; in Germany against Nazi propaganda), cultural and social habits, and civil rights. Nevertheless, the Convention on Cybercrime claims to provide a universal definition of "cybercrime" and other related terms and recommends global legislation to help protect against cyber offenders.

The Internet and its technology affect not only its users (as potential victims or alleged perpetrators) but also all non-users because it affects each member of society. According to the Council of Europe,

- Individuals and businesses are exposed to fraud just by using the Internet
- Hackers can "steal" bank details by hijacking legitimate systems – for instance, by inserting pages where the client is asked to give personal data which can then be used to gain access to their cash
- Children can become the victims of Internet paedophile groups.
- Hackers can threaten lives and businesses by disabling systems with "denial of service attacks." Spam is not just a nuisance but can be life-threatening if it blocks essential systems in hospitals or emergency control centres; it can also lead to the loss of millions of Euros for businesses.
- Racists and fascists often disseminate racist materials through their websites or spam e-mails.[33]

---

[32] (Self-regulation of ISP does seem to be working and further complications have been predicted). Gerlach 150.

[33] Council of Europe, *The Council of Europe and Cybercrime. Factsheets updated 24 November 2008*. 1 April 2009 < http://www.coe.int/t/dc/files/themes/cybercrime/default_en.asp>.

Cybercrime is a trans-national issue and I am sceptical that the Convention on Cybercrime will be able to handle this difficult widespread task. Nations that have signed and/or ratified the Convention differ in terms of their forms of democracy, economic development and technology. In addition, these states represent a variety of cultures and social norms (i.e. each of the North American, European, Asian, Western and non-Western countries is based on its own history of social, political and military evolution). In our contemporary postcolonial world, there are publicly recognized centers of economic power and strong/weak democracies; nations also behave differently in terms of their economic and demographic strategies. It is therefore problematic to apply the global guidelines of the Convention on Cybercrime to a variety of nations, each with their own regional and local peculiarities (different socio-economic rules, different forms of democracy, different types of cybercrimes at different levels of development, and different degrees of regulating privacy and human rights).

On the one hand, the Convention on Cybercrime has controversial points of view regarding human rights and civil rights. The privacy rights are addressed in terms that are rather general and vague, while at the same time the Convention is very detailed about search and seizure of computers, and retention of private information from users; it shows little regard for the protection of user privacy; it gives power to those countries which ratified the Convention to retain data and private information, despite the fact that a major concern of users worldwide is information privacy.

On the other hand, as I have previously observed, the Convention is too general about other types of cybercrime such as copyright and child pornography. There are dedicated laws which deal with copyright issues (e.g., the Universal Copyright Convention signed in Berne), or Intellectual Property ones (e.g., the Convention establishing the World Intellectual Property

Organisation signed in Stockholm, or Trade Related Aspects of Intellectual Property Rights, the TRIPS Agreement) which are much more complex and detailed than this convention and I cannot see any reason to rescind these laws due to a new regulatory act (The Convention on Cybercrime) which is much vaguer and general than these particular laws. Each country has laws and regulations regarding child pornography, largely based on the Convention on the rights of the child – 193 countries ratified it in December 2008. That these countries should somehow change these local regulations to accommodate the Convention's stipulations which, again, are not very strong, would make the fight against computer-related crimes weaker and less efficient. As an example, the Convention criminalizes the possession of pictures with children which do not necessarily involve a real person, a real child, because nowadays the images could be edited and adjusted in many ways. My point is that both Copyright/Intellectual property and Child pornography are issues too complicated to be treated in vague terms in few Articles in a general Convention on Cybercrime.

Another aspect of this Convention is the way it deals with mutual assistance and dual-criminality. No country should require mutual assistance when there is no dual criminality legislation between those particular two countries. A country should not be empowered to retain data or privacy information from a supposed criminal for a particular action when that action is not considered a criminal act in that particular country, in essence violating his/her privacy by retaining data and private information. The retention of data could be done when, in both countries, the person's action is considered as a criminal act under their legal systems. Also, the retention of information should be done accordingly to a specific level of authorization, such as the orders of a judge, not just based on this Convention on Cybercrime. The Convention extradition provisions should not replace the original binding Extradition treaties between two

countries, if any, because those provisions in the Convention are again too vague to adequately replace dedicated and elaborated Extradition Treaties. One reason Canada did not sign the CC is that the Canadian government does not want to have extradition clauses or rules with countries with which they do not yet have an Extradition Treaty (because of their differences in legislation, democracy or human rights). The Convention should not serve as the only extradition treaty between two countries which have no other extradition agreements in place.

I believe that the Convention on Cybercrime should focus on computer attacks such as viruses, hacking, and spam, its main goal being international cooperation in investigating those crimes, without having controversial provisions which contravene human rights by allowing for extradition and the violation of personal information privacy protection through data access, search and seizure, and information storage. As it stands, these provisions have helped to increase the surveillance power of those governments which used the Convention in an extreme way, such as Romania, where the government monitors and retains all communication traffic over phone, email and internet as a preventative measure in combating cybercrime. In my opinion, the Convention should address the offences which are unique to computer networks and computer systems and not attempt to mix technical issues with issues of human rights, copyright and intellectual property, child pornography, and extradition because these areas are already regulated by well-defined laws.

In addition, new measures to enforce laws and regulations regarding cybercrime should be put in place. A balanced approach is necessary in sensitive domains such as personal information privacy, and governments should be encouraged by the Convention to protect fundamental human rights. Also a reasonable approach should be taken into consideration when proposing the surveillance of a state's citizen

European and international experts collaborated to design the Convention on Cybercrime and its regulatory objectives. They were intended to harmonize domestic criminal laws with new laws against global cybercrime, to provide procedures for dealing with cybercrime, and to establish effective international cooperation for fighting against cyber offences. Eight years after the opening of the signature list and six years after the Convention's ratification, the aims of this convention are still being pursued.

"Cybercrime" has no stable definition and is a borderless phenomenon with transnational offenders. The model of global Internet regulation as proposed by the European Convention on Cybercrime includes some problematic relationships between each state's collective regulatory, economic and political organizations, and each citizen's individual self-regulation. Besides, different socio-economic and political cultures exists, not only in the Western world (with its developed countries based on long-term democratic regimes) and the Eastern world (the so-called non-Western world, including developing countries) but also in Western European nations and Eastern European nations (which are still overcoming the lingering effects of communist dictatorial regimes). Globally harmonizing Eastern and Western cybercrime legislation is an objective that is difficult to achieve because social habits, economic policies, technology, and socio-political organizations differ in the East and the West. The Convention on Cybercrime recommends that its articles to be applied to local legislation, but the local infrastructure and rules may differ in different countries.

My initial research has pointed to this chapter's conclusions: Internet crime must be regulated, but the Convention on Cybercrime cannot be applied everywhere in the same way. The state, state agencies and institutions which apply public policies on cybercrime, offenders and

victims, and the global society are intended to act as a whole trying to cope with transnational borderless Internet-related crimes. However, national states have various economic systems (e.g., neo-liberal market-based or socio-democratic state-based governance systems), political systems (e.g., federations or republics) and distinct policy choices for the role of their democracies (e.g., liberal or socially-protective policies).[34] According to the author Joel Reidenberg, specific laws could be harmonized, but doing so would be harmful, and new strategies are needed. Furthermore, the socio-political organization and technological features of each national state are very complex and the concept of democracy has its own limitations. A democracy can be strong or weak, and "measured" and "scaled" in terms of safety, equality and electronic media usability.[35]

The Convention on Cybercrime can evolve and change gradually as an offline changing body of rules and legal recommendations as long as the Internet, technology, and its users develop better online professional skills. More time may be needed to implement the Convention correctly, or as it was intended to be implemented. Other controversial international treaties have been difficult to implement globally due to differences in local legislation and cultures. For example, some treaties refer generally to human rights, where others refer specifically to women's rights. [36]

---

[34] See Joel Reidenberg, "Resolving Conflicting International Data Privacy Rules in Cyberspace," *Stanford Law Review* 52.5 (2000): 1315-1371.

[35] For a fascinating study of democratic utopias and the politics of cyber space, see Diane Saco, *Cybering Democracy: Public Space and the Internet* (Minneapolis: University of Minnesota Press, 2002).

[36] For example, see the Convention on the Elimination of All Forms of Discrimination against Women (CEDAW), which was adopted in 1979 and entered into force in 1981. *Convention on*

Online cybercrime and its offline legislation characterized by the blurring of private/public and national/international have unlimited possibilities. According to Peng, "there will not be one universal model for regulating the Internet." [37] This conclusion applies to the international community trying to accommodate the national differences based on the culture of each national state, which is not possible in practice.

---

the Elimination of All Forms of Discrimination against Women: Reference Document (Ottawa: Dept. of the Secretary of State, 1986).

[37] Peng "How Countries."

Chapter Two: Canadian Cybercrime and Its Regulation

In this chapter, I will discuss the Canadian political and economic systems, examining how the Internet is regulated in Canada and how the Convention on Cybercrime is influenced by the Canadian socio-economic and political context. Canada's democratic practices and its reasons for signing but not ratifying the Convention will be examined in this chapter.

The Canadian democracy is a strong and modern form of government within a federal frame[38] and operates according to the traditional meaning of *democracy* (i.e., a form of government informed by the rule of the *demos*, that is, of the people, "where 'people' designate the popular masses (in contrast to social or economic elites").[39] A federation composed of provinces and territories, Canada has a parliamentary government, a parliamentary democracy and a constitutional monarchy; the criminal law of Canada is under the exclusive jurisdiction of the federal government, and laws are stipulated in the Criminal Code of Canada.[40] In 1867, the Constitution Act became the main piece of legislation for organizing the parliament. The power to enact criminal law is derived from the Constitution Act as follows: section 91 refers to the federal powers, and section 92 refers to provincial legislative competence.[41] Canada's liberal democracy is based on the principles of representative democracy (the election of a small number

---

[38] For a fascinating discussion of the ideology of the Canadian Confederation, see Samuel LaSelva, *The Moral Foundations of Canadian Federalism: Paradoxes, Achievements, and Tragedies of Nationhood* (Montreal, Québec: McGill-Queen's University Press, 1996).

[39] Andrew Levine, *Political Keywords: A Guide for Students, Activists, and Everyone Else* (Malden, MA: Blackwell Publishing, 2007) 43.

[40] See Eugene Forsey, *How Canadians Govern Themselves.* 6th ed. (Ottawa: Library of Parliament, Public Information Office, 2005).

[41] Gerlach 71-72.

of representatives by the citizens as a whole) and the traditional values of liberalism: civil rights and natural rights that are inscribed in a constitution.[42]

Furthermore, in Canada, the proposed Democracy Institute [43] would have a professional preoccupation with strengthening democracy and with establishing itself as a national institute for gathering information, promoting abroad and advocating the consolidation of democratic governments within nations. Such an institute indicates that Canadian democracy is in an advanced phase and also shows the degree to which democracy has developed in Canada in comparison with other countries.

A key feature of Canadian democracy is multiculturalism, which has shaped Canadian law in accordance with ethnic, racial, and religious diversity, transforming the mosaic social structure into a harmonious framework with effects on legislation and people's rights.[44] The deep cultural diversity and pluralism of Canadian minorities is a challenge for the government. As a side effect, Canada has a general criminal law applied to all Canadian citizens.

Democracy as a form of socio-political government is closely related to the economic principles and values of liberalism. This refers to the belief in "the political equality of all mature

---

[42] David Robertson, *The Routledge Dictionary of Politics*, 3rd ed., (London: Routledge, 2004) 281.

[43] Thomas Axworthy, Leslie Campbell and David Donovan. *The Democracy Canada Institute: a Blueprint* (Montreal, Quebec: Institute for Research on Public Policy = Institut de Recherche en Politiques Publiques, 2005 Gibson Library Connections, 2008).

[44] For more about Canada's history and multiculturalism policies (e.g., the Canadian Multiculturalism Act, 1985), see Jean Kunz, *From Mosaic to Harmony: Multicultural Canada in the 21st century: Results of Regional Roundtables* (Ottawa, Ont.: Policy Research Initiative, 2007 Gibson Library Connections, 2008).

individuals" linked to institutional mechanisms and "above all, the free market."[45] The personal skills and merits of free individuals are central to the system; state intervention is a problematic issue because it brings up a confrontation between the private and public sectors. The contemporary political and economic systems are governed by a neo-liberal public policy and state regulations. Thus, private rights, the public good, and the public interest are represented and protected by the state.

Canada's mixed economy is underpinned by the classical values of *laissez faire* liberal ideology and a welfare state policy.[46] As a liberal democratic capitalist society, Canada implemented a federal neo-liberal policy in late the 1990s. One of the neo-liberal objectives is linked to the communication domain. As the author Andrew J. Reddick has argued, when discussing Canada's new information policy for the 21st century, the development of the information domain is part of Canada's national policy and industrial achievements:

> For example, the Action Plan goals for Canada's Information Highway include objectives of 'creating a competitive, consumer-driven policy and regulatory environment that is in accord with the Canadian public interest and that is conducive to innovation and investment by Canadian industry in new services on the Information Highway, 'and' realizing the economic and social benefits for all Canadians of the Information Highway and allowing them to participate fully in the emerging Information Society.'[47]

---

[45] *The Oxford Companion to Politics of the World* (Oxford: Oxford University Press, 1993) 222. Modern liberal democracies justify the sovereign power of the state and are against the principle of a single-party system.

[46] See Diane Jurkowski and George Eaton, eds., *Between Public and Private: Readings and Cases on Canada's Mixed Economy* (Concord, Ont: Captus Press, 2003).

[47] Reddick 128.

As a consequence, the development of the information industry and new communication technologies provided new facilities for users of the Internet, but also generated a new category of offences and offenders: cybercrime and cyber-offenders, respectively.

In terms of Canada's regulations of Internet crime, some scholars have studied the relationship between economic rights and democratic rights, concluding that the Canadian government's perception of the "public interest" is narrowing, showing the limitations of the neo-liberal policy in relation to the Internet. For example, in 1994, the Canadian government launched the Canadian strategy for the "Information Highway," establishing the Information Highway Advisory Council (IHAC) in order to implement new media such as the Internet, to help advance the information industry and to facilitate affordable access to all users, etc. Privacy protection and network security were also main objectives of the IHAC's strategy.[48] Interestingly, one of the IHAC's findings and recommendations referred to minimizing regulations in order to obtain economic advantages within Canada's private industries. Moreover, in 1998, Industry Canada and Justice Canada, working as a task force, initiated a project to help advance Canada's entry into e-commerce.[49]

Even though the economic aspect of the Internet is a limiting factor in Canadian Internet regulations, Canada has carried out governmental initiatives to regulate the Internet. As Natascha Gerlach notes, broadcasting and telecommunications in Canada fall under federal jurisdiction.[50] Thus, regulatory powers related to communications also fall under federal jurisdiction and can be applied to new information technologies such as the Internet.

---

[48] Gerlach 89-95.

[49] Gerlach 96-102.

[50] Gerlach.

For instance, starting in the 1990s, public debates have occurred about new media and Internet regulation input for all Canadian users in relation to affordable access to information technology, privacy and so on.[51] Later, in 1999, the CRTC announced that after public consultations and Internet industry discussion, "the CRTC has decided there is no need to regulate the Internet."[52] Interestingly, ten years later, in 2008, due to the rapid growth of new media (e.g., the YouTube phenomenon), the CRTC recommended "harmonization of rules for broadcasting on television, and over the Internet and cell phones."[53] The activity regarding the Canadian legislation that could be applied to new technologies and the Internet was not coherent. The main issue was how to apply existing traditional laws to the Internet. At the beginning, during the 1990s, it was not clear if the Internet was a "criminal" or "privacy" issue. Then, as cybercrime became a global issue due to the borderless nature of the Internet, Canada started to look for a way to respond. In 1994, a non-governmental initiative took place in order to deal with Internet-based offences: the so-called Cyber Tribunal. More like an "electronic tribunal-school" than an effective program, it was launched on cyberspace by a professor in Montréal aiming to

---

[51] The CRTC is the Canadian Radio-Television and Telecommunications Commission, the regulatory body responsible for implementing public policy in broadcasting and telecommunications. "The CRTC Examines Internet Regulation and Issues in Canada," 14 August, 1998, 4 January 2009 <http://canadaonline.about.com/library/weekly/aa081498.htm>.

[52] "Canadian Government Will not Try to Regulate the Internet," 22 May 1999, 4 January 2009 <http://canadaonline.about.com/library/weekly/aa052299.htm>. Some of the reasons for not regulating the Internet were "existing Canadian laws, as well as industry self-regulation, content filtering software and media awareness are appropriate tools to deal with illegal and offensive content," "71 per cent of all Web sites are American," and "5 per cent of content on the Internet is Canadian."

[53] "Harmonize Rules for Internet, TV, CRTC Told," 9 September 2008, 4 January 2009 <http://www.cbc.ca/arts/media/story/2008/09/09/new-media.html>.

arbitrate e-commerce disputes while involving students. The experimental Cyber Tribunal now has two versions, and some of its results were applied in Europe, where it offers to "European consumers an electronic platform for resolving disputes with online retailers." [54] The Cyber Tribunal is a negotiation and mediation platform that was made available throughout Europe in October 2001, exactly a month before the European Convention on Cybercrime was signed in November 2001.

Before Canada signed the Convention on Cybercrime, public debates about computer-related crimes occurred frequently and were very precise, pointing to the lack of legislation within this crime area. For example, in 2000, according to a survey by a United Nations-sponsored network of Internet policy officials, Canada, along with other countries, had to update its Criminal Code to include new cyberspace crimes and, thus, to implement cyber laws.[55] Moreover, the study warned that " unless crimes were defined in a similar manner across jurisdictions, coordinated international law enforcement would remain very difficult, posing serious threats to global information lifelines.…"[56] The suggested international law framework for fighting against cyber offences was referred to as the European Convention on Cybercrime.

---

[54] Professors Karim Benyekhlef and Pierre Trudel at the University of Montreal's *Centre de recherche en droit public* launched this online institution project in order to verify "the hypothesis that Internet functions can be used to resolve disputes arising online. In particular, the project targeted consumer disputes arising between users and online retailers." The hypothesis was verified. More details are available at www.cybertribunal.org 20 April 2009.

[55] The cyber offences covered by the survey were data-related crimes, including interception, modification and theft; network tampering, including interference and sabotage; crimes of access, including hacking and virus distribution; and computer-associated crimes, such as aiding and abetting cyber criminals, computer fraud and computer forgery. Chu Showwei, "Canada is a Laggard in Enacting Laws to Crack Down on Cybercrimes,"*Globe and Mail* 14 December 2000, 23 January 2009 < http://www.infosecnews.org/hypermail/0012/3233.html>.

[56] Showwei.

The Convention on Cybercrime represents one approach trying to regulate the Internet globally. The recent history regarding the potential implementation of the Convention in Canada has generated a strong public debate. Canadian officials, as well as other official representatives of the countries involved in drafting the Convention's sections and articles were called on to make observations and give content input before Canada signed the Convention. For example, in 2000, the Hon. Anne McLellan, Minister of Justice and Attorney-General of Canada, asked the Information Technology Association of Canada (ITAC) to contribute to draft 19 of the Convention proposal. Mr. Gaylen Duncan, the then president and CEO of ITAC, welcomed the initiative and appreciated the urgency of the topic, that is, "the problem of crime in cyberspace." [57] Still, he expressed some concerns after attending roundtables with the ITAC members, recommending that "Canada should not sign the Convention unless significant changes are made."[58] The ITAC's argument included the following points:

> While the ITAC accepts that new legislation addressing only cybercrime may be necessary in exceptional cases, the practice should be discouraged. The ITAC would prefer adaptation or extension of existing laws wherever possible. The introduction of parallel legislation for familiar crimes facilitated by computer use will only complicate legal processes.
>
> Portions of the draft convention that involve technology would have benefitted from earlier consultation with our industry. The absence of critical sections (in draft 19, at least) dealing with interception is a major weakness as interception has serious implications for both confidence in industry and individual privacy.
>
> The ITAC is concerned with the clear intention that the Convention serves as a group extradition treaty between signatories even those without bilateral extradition treaties for other forms of crime. It seems odd that cybercrime would be treated so differently, especially when the reason why Canada does not have extradition treaties with certain countries is that

[57] Center for Democracy and Technology. "International Issues: Cybercrime (Oct. 23, 2000)," 5 January 2009 <http://www.cdt.org/international/cybercrime/001023itac.shtml>.

[58] Center for Democracy and Technology. "International Issues: Cybercrime."

> their justice systems are perceived as insufficiently just. We would not want to see Canadians extradited to such a country just because it had signed the Convention.[59]

The ITAC pointed out some sensitive issues: the notion of privacy in the case of interceptions of Internet messages, and the legal rights of Canadian citizens in cases of potential extradition to countries with which Canada does not have extradition agreements. Finally, some of the arguments were communicated to the Council of Europe on behalf of the Canadian state, and some of them were incorporated into the Convention on Cybercrime's final draft. Canada signed it on November 23, 2001, but has still not ratified the Convention.

Canada recognizes that Internet-based offences represent a major issue. The Canadian Centre for Justice Statistics has reported on the issue of Cybercrime – its terminology, statistics and federal legislation – and collected data to compare computer-related crimes in Canada, Great Britain and the United States to draw conclusions.[60] This 2002 report stated, "Similar to research findings, consultations with Canadian police indicated that a uniform definition of cybercrime has not been established among the police community," and that not all 11 major police forces in Canada have "a specialized unit that is responsible for investigating cyber-crimes and have developed definitions, policies and procedures to assist in the investigation."[61] A cyber offence, in this case, is defined either as "a criminal offence involving a computer as the object of the crime," or "the tool used to commit a material component of the offence."[62] Some synonymous

---

[59] Center for Democracy and Technology. "International Issues: Cybercrime."

[60] For instance, see Melanie Kowalski, *Cyber-Crime: Issues, Data Sources, and Feasibility of Collecting Police-Reported Statistics* (Ottawa: Canadian Centre for Justice Statistics, 2002).

[61] Kowalski 5.

[62] Kowalski 5.

phrases are used interchangeably by the Canadian police when referring to cybercrime: "computer-supported crime," "computer crime," "computer-related crime, "high-tech crime," "cyber-crime" and "Internet crime."[63] The Canadian Centre for Justice refers to Canada as "one of the first countries to enact criminal laws in the area of computer crime,"[64] emphasizing the attention paid in Canada to child pornography. As well, to help prevent and detect computer-related crimes, Canada has federal bodies such as the Office of the Critical Infrastructure Protection and Emergency Preparedness (OCIPEP), and some "major national initiatives are in place that address concerns regarding offensive and illegal content on the Internet," such as the Federal-Provincial-Territorial Working Group on Offensive Content.[65]

As we have seen, Canada has federal initiatives and regional institutions aiming to regulate the Internet in accordance with the Convention on Cybercrime, even though Canada has not ratified this international treaty. When a country signs an international treaty or a convention, that country expresses its support for the general principles included in the legal framework as well as the intention to be legally bound by it. A convention does not become legally binding in a country until the country ratifies it. Once a country ratifies a convention, the country is legally bound to the convention's articles and its international implementation. Thus, the convention has jurisdictional powers among the ratifying states. Some Canadian governmental representatives have criticized "Canada's inaction on cybercrime."[66] More specifically, at a conference on

---

[63] Kowalski 6.

[64] Kowalski 7.

[65] Kowalski 9-10.

[66] The identity theft conference was hosted by the B.C. Freedom of Information and Privacy Association on November 24, 2008. See Gillian Shaw, "Canada 'Reputed to be Lax on

identity theft that took place in Vancouver in November 2008, Canada's Privacy Commissioner, Jennifer Stoddart, said, “We don't have anti-spam legislation, we don't have adequate Criminal Code provisions for identity theft fraud, we don't have mandatory data breach provisions.”[67] Moreover, Stoddart made unexpected comments when comparing the impact of the international drug trade to the international personal information trade: "This is a shocking phenomenon to think that the international drug trade is now less lucrative than the trade in personal information;" she also added that cybercrime phenomenon does not get nearly the same attention from police and law enforcement agencies as the drug trade. Stoddart concluded that “much more is needed to inspire consumer trust than a few legislative changes.” [68]

Besides the fact that Canada does not apply the Convention on Cybercrime due to legislative issues (i.e., privacy) the official representatives think that Canada’s current laws may not be enough to regulate the online commerce. In addition, some cybercrime researchers recommend the ratification of the Convention on Cybercrime by the Canadian government in order to internationally combat and fight against specific Internet crimes (i.e., child pornography).[69] In her 2008 PhD thesis, Sara M. Smyth strongly recommends that the Canadian

---

Cybercrime',“ *Times Colonist* 25 November 2008. 20 Jan. 2009 http://www.timescolonist.com/news/Canada+reputed+cybercrime/991226/story.html.

[67] Shaw.

[68] Shaw.

[69] Smyth.

"Parliament ratify the Convention and work with other nations to pursue a common criminal policy."[70] According to Smyth,

> The main thrust to the Convention is to require participating states to enact legislation granting broad search and seizure powers to law enforcement authorities, including the power to compel the Internet Service Providers (ISPs) to intercept data transmissions, to provide assistance to police in the storage and search of data transmissions, and to provide information about their individual customers to police.[71]

This requirement necessitates harmonizing the ISPs for data transmission as well as updating Canadian laws even though this Convention's stipulations are against the interests of private users. Satisfying this requirement could lead to ethical problems and conceptual discussions relating to the notion of "privacy," which is inscribed in the constitution as part of human rights. Smyth claims:

> Canada has not yet ratified the Convention largely because it has not been able to draft workable data retention rules including preservation orders, which the Convention requires signatory states to adopt. Critics of the Convention have argued that privacy interests of individual users are undermined by the interception and recording of data. However, the Convention's procedural requirement to enable the real-time interception of data can be implemented in accordance with Canada's existing privacy laws, as well as the *Canadian Charter of Rights and Freedoms*….[72]

Another important point of discussion involves technology and legal jurisdiction. Some technical difficulties would have to be overcome in order for the Canadian jurisdictional police to be able to retain online data, because even if the police had jurisdictional power, the ISPs are not required to contain interception capabilities. Also, Smyth recommends that the Canadian Parliament enact legislation to allow preservation orders of retaining private

---

[70] Smyth 12. She proposes a sophisticated three-tiered regulatory model in order to regulate the Internet effectively in relation to child pornography. Some of her recommendations are mentioned here.

[71] Smyth 13.

[72] Smyth 14.

information (which are stipulated in the Convention on Cybercrime). Smyth concludes that the European Union and the United States have legislative tools for ISPs interception and can serve as a model for Canadian policy makers while safeguarding privacy rights and guarantees. Canada's laws can be harmonized with other legal jurisdictional rules in the Western world. Canada has to consider that its complicated system of privacy bylaws can further complicate the ratification of the Convention on Cybercrime.

Canada has advanced technology (which gives citizens easier access to political institutions[73]) as well as a high cybercrime rate, according to the Center for Democracy and Technology and Canadian Centre for Justice Statistics. The practice of democracy is thought to be enhanced when the communication between citizens and governments is improved and transparent due to the development of information communication technologies (ICTs). According to the 2008 Saskatchewan Institute of Public Policy, e-democracy, that is, e-government and e-governance through an online political agenda and institutionalized systems, actually exists in Canada, increasing the citizens' democratic participation and the transparency of the decision-making process. As Kathleen McNutt, Assistant Professor at the University of Regina, and Meaghan Carey, a Master of Public Administration candidate at the University of Regina, have observed:

> The e-government policy agenda in Canada is well established, currently providing secure access, various types of online transactions (income tax services, applications for student loan, change-of-address forms, etc.), and public access to government information.[74]

---

[73] Pierre-Léonard Harvey, *La Démocratie Occulte: Rapports de Force, Gouvernance et Communautique dans la Société de l'Information* (Québec: Presses de l'Université Laval, 2004) XiV.

[74] Kathleen McNutt and Meaghan Carey. *Canadian Digital Government* (Regina, SK, Canada: Saskatchewan Institute of Public Policy, 2008) 1.

The relationship between the role of the state and the economy and the implications of technology and commerce within the Internet are challenging new topics for research. The results of the new technology, such as e-taxation, e-regulation and e-governance, raise issues involving public morality, criminality, and the prevention of cyber fraud.[75] Since Canada has a strong economy and sophisticated technology, it has the ability to regulate its electronic market and protect consumers and copyright, without implementing the Convention on Cybercrime. Canada has a developed Global Information Society (GIS), a strong democracy, and multiculturalism. However, Canada signed the Convention on Cybercrime but did not ratify it because it seems to be difficult to harmonize federal cybercrime legislation with human rights.

[75] C. Satapathy. "Role of the State in the E-World," *Economic and Political Weekly* 35.39 (2000): 3493-3497.

Chapter Three: Romanian Cybercrime and Its Regulation

In this chapter, I will discuss the Romanian political and economic systems, and examine how the Internet is regulated in Romania and how the application of the Convention on Cybercrime is influenced by Romania's socio-economic and political context. In the context of Romania's recent democratic practice, I will also examine why Romania, unlike Canada, has signed and ratified the Convention on Cybercrime.

The Romanian capitalist democracy is new and fragile. In 1989, the Romanian national state, an ex-socialist republic from the Eastern European block,[76] overthrew the communist dictatorial regime of Ceausescu.[77] After almost twenty years of transition from dictatorship to democracy, and from a centralized state-controlled market to a liberal market economy,[78] the Romanian state became part of the European Union in 2007.[79] As such, Romania had to satisfy

---

[76] Before the Second World War, Romania was a modern constitutional monarchy. The Socialist Republic of Romania was established in 1947, following the Yalta Conference Agreement at the end of the Second World War held in Crimea in February 1945.The Yalta Conference sealed the postwar Yalta Agreement through which Europe was split into zones of influence; Romania became subject to the communist socialist and military Soviet occupation. For more details about the Yalta geopolitics, see Alexander Yakovlev, ed., *The Yalta Conference, 1945: Lessons of History* (Moscow: Novosti Press Agency Pub. House, 1985).

[77] For more details about the life of the Romanian people under Soviet occupation and especially under the communist socialist regime of Ceausescu and its alienating ideology see, Katherine Verdery, *National Ideology under Socialism: Identity and Cultural Politics in Ceausescu's Romania* (Berkeley: University of California Press, 1991).

[78] For an insightful overview of Romania's transitional phase to a democratic system, see Ion Iliescu, *Communism, Post-Communism and Democracy: the Great Shock at the End of a Short Century*, Interviewed by VladimirTismaneanu (Boulder: East European Monographs; New York: Columbia University Press, 2006).

[79] The efforts and reforms made by Romanian governments to implement the accession criteria to EU, before becoming a real member of the European Union, have been analyzed many times. Romania's geostrategic importances in Europe have mattered ever since Romania became a

new economic, political and legislative requirements in order to be integrated into the EU framework.

Many reforms in justice, industry and environmental policies have been started. Many challenges have been faced by Romania's newly emerged democratic institutions and allegedly free-market economy. New technologies had to be developed within a liberal economic structure, but after 1989 the Romanian economy suffered from major structural and functional disruptions, and as a result the technological development was modest because the state's communist economy had been based on heavy industry (e.g., mining, car production, steel industry) and was underdeveloped and inefficient. However, after the year 2000, and after Romania's 2007 accession to the EU, the Romanian economy quickly expanded mainly because of private foreign investments and local private initiatives.[80] Thus, new technologies were developed and the Internet became a common tool in urban areas, offering a broader connection with the global world.

The Romanian capitalist market developed economically and technologically and the social transformations generated new social classes and habits that now coexist with the old ones. A specific feature of contemporary Romanian society is the cyber criminal activity, which

---

NATO member on 29 March 2004. For a significant discussion of this topic, see Aurelian Craiutu, "*Romania: The Difficult Apprenticeship of Liberty (1989-2004)*," *East European Studies* lectures, Meeting Report 298, 9 June 2004, Woodrow Wilson International Center for Scholars, 3 Jan. 2009 http://www.wilsoncenter.org/index.cfm?topic_id=1422&fuseaction=topics.publications&doc_id=96456&group_id=7427.

[80]Romanian National Institute of Statistics, "GDP 2006," 7 April 2009 < http://www.insse.ro/cms/rw/core/search/search.ro.do;jsessionid=0a02458c30d597c08306e0b84774bba0943aae566bee.e38QbxeSahyTbi0Rchr0>.

seemed impossible in Romania 15 years ago. This issue is now recognized globally and locally and includes cross-border cyber offences and offenders.

In order to prevent and fight against computer-related crime, the Romanian state signed the Convention on Cybercrime on 23 November 2001 and adopted the Law 161/2003[81] to harmonize the national legislation with the provisions stipulated in the Convention. Title III from this Law refers to the prevention of and fights against cybercrime in corroboration with the Criminal Procedure Code and Criminal Code. Later, on 12 May 2004, Romania ratified the Convention, having already incorporated the provisions into the local legislative framework. Romania used the Convention as a guideline while implementing the Convention's articles one by one. Thus, the Romanian cybercrime legislation is compatible with international standards and defines cybercrime terminology (computer-system, computer data, service provider, traffic data, child pornography, data on the users/subscriber information) as it is stipulated in the Convention. Furthermore, Romanian cybercrime legislation offers additional information (e.g., on automatic data processing and computer programs), as can be seen in Romania's cyber profile drafted by the Council of Europe in 2008 (Appendix 2).[82] According to Romanian law, cybercrime has three

[81] The Law 161/2003, published on the Official Gazette no. 270 from 21 April 2003, contains significant provisions under Title III for preventing, discovering and punishing cyber offences. For a detailed analysis of cybercrime law enforcement in Romania according to the European Convention on Cybercrime, see Ionel Georgescu, "Infractiunile Informatice Prevazute de Legea Nr. 161/2003 (Cybercrimes according to the Law 16/2003)," *Buletin Documentar* 3 (2005) 7 pp. 3 January 2009 <http://www.pna.ro/text_doctrina.jsp?id=46>.

[82] This profile as of April 2008 can share information on cybercrime legislation and offer an assessment of the current state of Convention's implementation under national legislation. This material has as Appendix 1 Romania Law 161/2003 (Title III on Preventing and Fighting Cybercrime) and Criminal Code (Title II). See Alexander Seger, "Cybercrime Legislation - Country Profile - Romania," April 2008, COE, 2 May 2009 <

main categories: offences against the confidentiality and integrity of computer data and systems; computer-related offences, computer-related forgery and computer-related fraud; and content-related offences involving child pornography using computers.[83] The Romanian government appears to have taken all necessary legal measures to transfer the international Convention's provisions into local legislation. For example, article 1 of the Convention on Cybercrime (which defines terminology such as "computer system," "computer data," "service provider," and "traffic data"), article 9 (dealing with "child pornography") and article 18 (dealing with "subscriber information") are all covered by article 35 of Law 161/2003.[84] A difference between the Convention's stipulations and Romanian legislation regarding the intentional element of cyber offenses was observed by Alexander Seger, head of the Economic Crime Division of the Council of Europe, who noted that:

> Under the Romanian legal system, an act that resides in an action committed with negligence shall be an offence only when the law provides this expressly (article 9 paragraph 2, Criminal Code). As a result of this provision, it was stated that there is no need to specify expressly the intentional element in the text.[85]

This shows that international conventions can be subject to modification by local legislation, since these local laws are more applicable in practice to that specific country (e.g., Romania). The international cooperation procedures in criminal matters are stipulated in Law 302/2004 (which deals, for example, with extradition and transfer of proceedings in criminal matters). Even

---

http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/CountryProfiles/default_en.asp>.

[83] Iinfringements of copyright are partially covered by Law 8/1996 on copyright and additional rights. Georgescu.

[84] Seger, "Cybercrime Legislation - Country Profile - Romania" 1.

[85] Seger, "Cybercrime Legislation - Country Profile - Romania" 1.

though Romania made efforts to adapt the Convention on Cybercrime to the local Romanian legislative framework, some Romanian cybercrime professionals argue that "Law no. 161 of 2003 represents a start, but for keeping up with huge criminal diversity that takes place with a simple keyboard and with a simple click of the mouse, legislation should not stop here."[86]

The Romanian political and economic systems are governed by a marked-based public policy. Some Romanian scholars have studied the relationship between Romanian democracy and the implementation of cybercrime legislation with help from international institutions.[87] For example, the US government shared its expertise with the Romanian state in order to provide theoretical and practical information on cybercrime. In September 2004, one year after Law 161/2003 had been enacted, the US Ambassador, Dr. Jack Dyer Crouch II, and the Romanian Minister of Communications and Information Technology, Adriana Ticau, launched the "*Handbook for the Enforcement of Legal Provisions Regarding Informatics Crime*" in order to provide a useful guidebook for cyber law enforcement, for citizens as well as for private companies. This guide has two sections, one referring to informational systems and technologies, the other one to local and international cyber law enforcement and frameworks. Dr. Crouch declared:

> The implementation of this legislation to combat computer crime by the government, but also to legally pursue cyber offenders, contributes to enhancing the trust between the United States and Romania. This is why, during the last three years, we have supported the Information Technology Initiative in Romania (RITI) and we have spent over a

[86] Georgescu.

[87] See Romania, Ministerul Comunicatiilor si Tehnologiei Informatiei (Ministry of Communications and Information Technology). *Ghidul pentru Aplicarea Dispozitiilor Legale referitoare la Criminalitatea Informatica* (*Handbook for the Enforcement of Legal Provisions Regarding Informatics Crime*) (US Embassy in Bucharest, USAID and RITI, 2004.) 6 January 2009 < http://www.mcti.ro/index.php?id=216&L=2>.

> million dollars on various projects for Romania to become part of a global information society. Cybercrime is not a problem specific to Romania, we have such phenomena in the United States too.[88]

Furthermore, Dr. Crouch stated that the Romanian Ministry of Communications and Information Technology "has done" a great job developing portals through which government activities increase efficiency and transparency and the ability to conduct electronic transactions as an important tool to combat corruption."[89]

Romania has basic technology and a high cybercrime rate, according to the Center for Democracy and Technology. Most of the cybercrimes committed by Romanian offenders are linked to fraud, possibly because of the low quality of life and low incomes in Romania. For example, Virgil Spiridon, Director of the Department for Cybercrime (DCCI) of the General Inspectorate of the Romanian Police, declared that during the first eight month of 2008, almost 900 cases of internet fraud had been reported in Romania.[90]Most of the reported crimes involved fake online bids, phishing, identity theft, and cloned credit cards, and were committed by Romanian offenders in collaboration with international criminal networks. According to Spiridon, the main difficulty in detecting cybercrime relates to the transnational character of computer crimes and the advanced pace of technology, which requires the police to be

---

[88] "Cybercrime," *Market Watch* 8 September 2004, 6 January 2009 <http://www.marketwatch.ro/articol/263/Criminalitatea_informatica/>.

[89] "Cybercrime."

[90] AFP, "Romania - a Country that Fights Against Cybercrime," 24 November 2008, 6 January 2009 <http://www.euractiv.ro/uniunea-europeana/articles%7CdisplayArticle/articleID_15579/AFP-Romania-o-tara-care-se-lupta-cu-criminalitatea-informatica.html.

continuously informed about the sophisticated methods being used by cyber criminals.[91] The economic cyber offences committed by Romanian-born citizens caused the small town of Ramnicu-Valcea to become known internationally as "the world capital of cybercrime." The famous Romanian hacker nick-named Vladut (Vlad Duiculescu) lived there. Vladut hacked into NASA's servers and was caught by Romanian officials with FBI support, along with almost 40 other hackers who were arrested in 2008.[92] The NASA hacker was accused of eBay fraud, and also of causing USD 1.5 million damages to NASA servers. Policing cybercrime creates ethical issues at the global level (e.g., the Romanian NASA hacker was wanted by IBM) and also privacy issues within a society recovering from almost fifty years of totalitarian surveillance. Another aspect of cybercrime, Spiridon noted, is the high rate of unemployed young people becoming involved in computer-related criminal activities. The poor economic conditions within a fragile democracy and a new market economy are closely linked to the degree of criminal activity in Romania. For instance, at a workshop on cybercrime held in 2008 in Sri Lanka, Alexander Seger stated that: "cybercrime is the most transnational of all crimes." Cristina Shulman, an official representative of the Council of Europe, ended her lecture on Romania as follows:

---

[91] Mainly for this reason, the Romanian police collaborate with the FBI and other international police bodies in order to fight against cybercrimes. AFP, "Romania - a Country that Fights Against Cybercrime."

[92]The Romanian town of Ramnicu-Valcea has almost 100.000 inhabitants and has a high rate of cyber offenders. See AFP, "Romania - a Country that Fights Against Cybercrime." The fight against criminal hacking activity is helped by a European programme called "Hackers Profiling Project (HPP)." Started in 2006 by the United Nations Interregional Crime and Justice Research Institute (UNICRI), HPP strives to create a global database of computer intruders. See UNICRI, "Cybercrimes - HPP," 3 May 2009 http://www.unicri.it/wwd/cyber_crime/hpp.php.

> Among the main tendencies identified that define the evolution of the transnational crime in Romania it is also increasing in cybercrime [sic]. The most common cybercrimes are: Internet fraud and electronic payment instruments fraud in view of fraudulent use.… It can be concluded that Romanian legislation meets the requirements of the Convention and has proved to be effective in practice. [93]

According to the COE representative, the most common Romanian cybercrimes are related to e-fraud that exploits computer vulnerabilities. However, although the national legislation seems to be effective on paper, Romanian cybercrime is increasing in practice.

The Romanian government and information professionals strive to share knowledge, information, and expertise on cybercrime. International cyber law enforcement and the significance of the Convention on Cybercrime have been explained and analyzed by lawyers, prosecutors and police professionals when addressing information system managers, legal forces, judicial bodies, law students, etc. In order to prevent and combat computer-related crimes, Romanian authors have written about taxonomy and legal terms, procedures, strategies, legal tools, communication and information technology (ITC) and privacy issues.[94] Cybercrime and criminal justice international workshops for investigators, prosecutors and lawyers have often

---

[93] See Cristina Schulman, "The Implementation of the Convention on Cybercrime in Romania," handout, Workshop on Cybercrime for Hon. Judges and Workshop for Investigators, Prosecutors and Lawyers (Colombo, Sri Lanka, 27-28 October 2008), 7 January < www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/cy_activity.../567-IF08-CRISTINA_SCHULMAN_HandOut.PDF>.

[94] See Tudor Amza and Cosmin-Petronel Amza, *Criminalitatea Informatica (Cybercrime)* (Bucuresti: Lumina Lex Publishing House, 2003); Ioana Vasiu and Lucian. Vasiu, *Prevenirea Criminalitatii Informationale (Cybercrime Prevention)*, (Bucuresti: Hamangiu Publishing House, 2006).

been organized either in Romania or abroad with Romanian participation to raise awareness and to promote and to share measures against cybercrime.[95]

Romania also takes part in international programs determined to help improve the effectiveness of judges, prosecutors and lawyers in their struggle against global computer-related crimes. In order to enhance and advance cyber security, Romania intends to create the first European e-evidence and cybercrime library providing electronic evidence as a major prosecution tool.

Started in 2008, the project "European Certificate on Cybercrime and e-Evidence" was funded by the European Commission in 2005 and is being developed by the United Nations Interregional Crime and Justice Research Institute (UNICRI) in European and South-American countries. The main objective of this project "is to provide technical training on cybercrime, electronic evidence and the corresponding legal framework, to judges, lawyers and prosecutors. At the end of the course, students will receive the first European Certificate guaranteeing their technical knowledge of electronic evidence and hi-tech crime." [96] The project has two phases (developing the syllabus and then teaching classes and courses) in order to train almost 1000 people to obtain the European Certificate, which signifies that a graduate has a basic knowledge of cybercrime and electronic evidence, including "its technical terms, its novelty, its volatility,

---

[95] For a workshop devoted to strengthen the capacity of Romanian and Bulgarian prosecutors in the case of cyber criminal activity, see APTI (Romanian Association for Internet and Technology, "Justitie in Era Digitala (Justice in Digital Era)," agenda (Timisoara, Romania, 4-5 December 2008), 10 May 2009 < www.apti.ro/webfm_send/19>.

[96]The courses will be delivered in 11 European countries (Belgium, Croatia, Cyprus, Estonia, France, Greece, Italy, Lithuania, Romania, Slovak Republic and Spain), and 3 Latin America countries (Argentina, Brazil and Venezuela). See United Nations. Interregional Crime and Justice Research Institute (UNICRI), "European Certificate on Cybercrime and Electronic Evidence," 3 May 2009 < http://www.unicri.it/wwd/cyber_crime/ecce.php>.

the widespread belief that it is easily manipulated."[97] At the beginning of 2008, the Romanian government signed a partnership for this project, which is now in progress.[98]

In Romania, a post-communist society which has not recovered from its totalitarian trauma and dictatorial surveillance, the privacy issue has generated intense public debates. A national debate is now occurring about Law no. 298/2008 in accordance with "the directive 2006/24/C.E. of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC." The new directive was drafted by the European Parliament in order to fight against terrorism.[99] Law no. 298/2008 has been adopted, but public opinion in Romania considers that this law violates human rights and that moreover, the Commission on Human Rights in the Romanian Parliament incorrectly authorized the drafting of this law. However, the role of the parliamentary Commission on Human Rights is only consultative, and the law was adopted.[100]

---

[97] United Nations Interregional Crime and Justice Research Institute (UNICRI), "European Certificate on Cybercrime and Electronic Evidence."

[98] Prompt Media, "Bucuresti: Certificat European privind Criminalitatea Informatica si Probele Electronice pentru Judecatorii, Procurorii si Avocatii Romani," 6 January 2009 <http://www.promptmedia.ro/stiri/1-stiri/7545-bucuresti-certificat-european-privind-criminalitatea-informatica-si-probele-electronice-pentru-judecatorii-procurorii-si-avocatii-romani->.

[99] Vlad Mixich, "How Much is Your Personal Data?," *Hotnews*, 22 January 2009 <http://www.hotnews.ro/stiri-opinii-5343895-cat-costa-datele-tale-personale.htm>.

[100] The same the directive 2006/24/C.E. of the European Parliament and of the Council of 15 March 2006 on the retention of data was transposed into local laws in Germany and Great Britain even if the public opinion objected. Mixich.

Romania has recently become part of the EU and has an undeveloped Global Information Society (GIS) and a weak democracy and national ideology. Romania signed and ratified the Convention on Cybercrime but only on paper because they have not fully implemented the conventions. The current Romanian cybercrime (i.e., the financial fraud which is prevalent due to the precarious Romanian economy) is part of a public structure where state Internet regulation and citizens' self-regulation are both weak.

Chapter Four: Regional Adoption of International Conventions

In this chapter, I discuss how the Convention on Cybercrime is being implemented in Canada and Romania, and analyse how the global model of Internet regulation is being applied regionally. Is this model effective in practice? I will look at these two countries' democratic and technological structures and their current differences. Both states have signed the European Convention on Cybercrime, but only Romania has ratified it. Each country has its own rationale for regulating the Internet in relation to the country's Criminal Code and political strategies. I will compare how Canadian and Romanian governmental agencies act and will try to explain their inner mechanisms.

The relationship between democracy and technology is important because democracy effects technological developments. The relationship between technology and privacy (which is related to national borders[101]) will be discussed. Canada, one of the most developed countries in the world, has a strong and enduring democracy, as was shown in Chapter Two. The rapid growth of Canada's information and communication technology (ICT) has attracted much interest:

> Statistics Canada has been actively monitoring this growth and, in recent years, has sought to illuminate several aspects of ICT- related phenomena from many angles. Whether it was the size, growth and significance of the ICT sector at issue, the penetration and use of ICTs by households and individuals, or business and government connectivity and engagement in e-commerce, efforts were made to shed light on them by way of sound quantification and analysis.[102]

---

[101] Reidenberg 1325-1332.

[102] Statistics Canada. *Canada's Journey to an Information Society* Catalogue no. 56-508-XIE 2003, 5 April 2009 <ht*p://www.statcan.gc.ca/bsolc/olc-cel/olc-cel?lang=eng &catno=56-508-X*> VII.

According to data provided by Statistics Canada, "Over half (52.8%) of Canadian individuals had used the Internet in 2000 and many (42.2%) had an Internet connection at home."[103] Moreover, in 2001, "close to one-quarter (23.7%) of all Canadian households had a high-speed Internet connection, representing nearly half of all regular home Internet users."[104] In contrast, in 2007, Romania was ranked last in Internet access in Europe, according to a Eurostat (European Data Statistical Support) study on "Internet Usage 2007, Household and Individuals." [105]Still, Romania, an ex-communist country with a recent transition economy, has experienced an unexpected growth of Internet usage, although the regional spread of Internet providers appears to be much more developed in urban areas than in rural ones.

The more technology that a country develops, the more cybercrime and cyber threats against ordinary Internet users are developed. By increasing access to goods and services, the Internet improves the quality of life, but the extraordinary advances in computer technology can also provide opportunities for new criminal activity. Internet technology, as one of the most democratic mediums in terms of accessibility for all people, empowers ordinary citizens.

The nineteenth-century socialist ideal of freedom, education and art for all can be achieved by the use of the Internet and computers. Business can be carried out globally due to the Internet. However, the more democratic a society is in terms of Internet accessibility, the more cybercrime is generated. As the Council of Europe has observed, Internet technology makes societies Internet-dependent and exposed to cyber threats:

---

[103] Statistics Canada. *Canada's Journey to an Information Society* 81.

[104] Statistics Canada. *Canada's Journey to an Information Society* 212.

[105] Maria Smihily, *Internet Usage 2007, Household and Individuals*, Eurostat, 7 May 2009 < http://epp.eurostat.ec.europa.eu/cache/ITY_OFFPUB/KS-QA-07-023/EN/KS-QA-07-023-EN.PDF>.

> The Internet has a tremendous impact on societies all over the world. According to ComScore Networks, in 1999 there were 300 million Internet users. This number doubled to 747 million by 2007.
> E-commerce is also taking off. According to the same source, Americans spent $143 billion online in 2005, and Europeans are beginning to catch up.
> The true globalisation of markets is made possible by the Internet. Potential customers are now available worldwide at the touch of a button. The same is true for the anti-globalisation campaigner, who can easily rally support through the Internet.
> Our reliance on the Internet makes societies vulnerable. The main risk is cybercrime....[106]

Thus, the Internet has a double dimension: it is both a useful tool for democratic societies wishing to increase access to information, and a criminal weapon against privacy, intimacy, and honesty. The issue of privacy and human behaviour in relation to local legislation against cybercrime has been debated in both Canada and Romania as was shown in Chapters Two and Three.

Different regional issues are related to privacy laws and privacy protection. In democratic Canada, the privacy of individual users appears to be undermined by the interception and recording of data and, therefore, the users' right to freedom, confidentiality, and integrity takes precedence over the need to detect cybercrime. In post-totalitarian Romania, people protested unsuccessfully against the adaptation of the European directive on the retention of data generated or processed in connection with the provision of publicly available electronic communication services or of public communication networks. Still, according to the Council of Europe,

> Societies need to be protected against cybercrime, but there must be freedom to use and develop information and communication technologies properly, and a guarantee that people are free to express themselves. ...
> The cybercrime convention is based on the principles of the European Convention on Human Rights. It is subject to a range of conditions and safeguards, which means that people's freedom of expression and their right to privacy will not be sacrificed.[107]

---

[106] Council of Europe, *The Council of Europe and Cybercrime. Factsheets updated 24 November 2008.*

The Convention on Cybercrime seems to create a paradox. On the one hand, the Convention claims to follow and value the European Convention on Human Rights, Freedoms and the Right to Privacy. On the other hand, the principles expressed in the same Convention seem to violate human rights. Ironically, on behalf of human rights, one can violate human rights and the right to free expression:

> The convention sets up procedures to make investigations more efficient:
> - Through the immediate preservation of computer data
> - By empowering authorities to request the hand-over of specific computer data
> - By allowing investigators to collect traffic data and intercept content in real-time[108]

The Convention on Cybercrime raises the same issue in terms of the right to privacy and freedom of expression that the notion of democracy raises theoretically (concerning the rule of a minority over a majority). Scholars have been studying these apparently contradictory theoretical issues, concluding that they generate more unsolved issues such as the ownership of consumer information. The question remains: can international privacy standards be developed for the Internet given the vast cultural differences between, for example, North America and Europe,[109] or, in our case, between Canada and Romania?

This question can be applied to the implementation of the Convention of Cybercrime in both Canada and Romania. As was shown in previous chapters, Canada signed the Convention on 23 Nov 2001, but did not ratify it even though some people were criticizing Canada's way of

---

[107] Council of Europe, *The Council of Europe and Cybercrime. Factsheets updated 24 November 2008.*

[108] Council of Europe, *The Council of Europe and Cybercrime. Factsheets updated 24 November 2008.*

[109] Caudill.

fighting against cybercrime. Romania signed it on 23 November 2001, ratified it on 12 May 2004, and began to put it into effect on 1 September 2004. The Council of Europe has argued that the Convention on Cybercrime is the best, even perfect model to be followed globally by all countries in order to fight against computer-related crimes:

> Cybercrime is one of the major challenges facing modern society. The Council of Europe believes its convention is an ideal way for governments to anticipate problems and resolve them, working together to create security for the citizens of Europe and beyond.[110]

However, even if the Convention is intended to be a perfect model and to offer an ideal method for global law enforcement, the Council of Europe acknowledges, "even if 99.9% of the 747 million Internet surfers were to use it for legitimate reasons, this would still leave 747,000 potential offenders."[111] As a result, its very existence as a model is compromised by unsolvable difficulties of scale.

In relation to cybercrime, both countries' extradition treaties are interesting subjects needing to be addressed. For instance, Romania has recently ratified the Protocols of Exchange of Instruments of Ratification for the U.S.-Romania Mutual Legal Assistance Protocol and the U.S.-Romania Extradition Treaty with the U.S. (8 May 2009), to where most Romanian hackers direct their criminal activity.[112] These agreements refer to judicial assistance and the simplification of the extradition papers and procedure, as Hillary Clinton has declared:

---

[110] Council of Europe, *The Council of Europe and Cybercrime. Factsheets updated 24 November 2008.*

[111] Council of Europe, *The Council of Europe and Cybercrime. Factsheets updated 24 November 2008.*

[112] Ministry of Foreign Affairs of Romania, *Remarks at the Signing Ceremony for the Protocols of Exchange of Instruments of Ratification for the US-Romania Mutual Legal Assistance Protocol and the US-Romania Extradition Treaty* 12 May 2009 < http://www.mae.ro/index.php?unde=doc&id=13446>.

> These twin agreements between the United States and Romania will allow police and prosecutors in both countries to employ state-of-the-art tools to cooperate more effectively to bring criminals to justice on both sides of the Atlantic. The agreement will form part of an important network of similar agreements that the United States is reaching with all the countries of the European Union.[113]

The case of the famous Romanian hacker Vladut (Vlad Duiculescu), mentioned in Chapter Three, is an example of how these conventions or international treaties are not applicable in practice because Romania refused to extradite him. In contrast to Romania, Canada has not ratified the Convention on Cybercrime, but has many extradition treaties, and, starting in 2007, the RCMP-Interpol website began listing the countries that have extradition treaties with Canada and among them is Romania.[114]

An important issue to be discussed is the possible measurement of the effectiveness of changes in the legislation of a country, changes in enforcement policies, or changes in the number or kinds of cybercrimes. For example, in Romania, after the implementation of the Convention on Cybercrime, a website for registering complaints against *e-frauda* (electronic fraud) and the Romanian Cybercrime Center was launched on the website of the Ministry of Communications and Information Technology[115] in order to

> address fraud committed over the Internet. For victims of Internet fraud, eFrauda provides a convenient and easy-to-use reporting mechanism that alerts authorities of suspected

---

[113] Ministry of Foreign Affairs of Romania, *Remarks at the Signing Ceremony for the Protocols of Exchange of Instruments of Ratification for the US-Romania Mutual Legal Assistance Protocol and the US-Romania Extradition Treaty.*

[114] Lloyd Duhaime, "Extradition from Canada," 2 May 2009 http://www.duhaime.org/LegalResources/CriminalLaw/LawArticle-99/Extradition-Law-Canada.aspx.

[115] Ministry of Communications and Information Technology, www.efrauda.ro 10 May 2009 < http://www.efrauda.ro/efrauda/admin/default.aspx?StartTab=0&lang=2>.

> Internet fraud. For law enforcement and [116]regulatory agencies at all levels, eFrauda offers a central repository for complaints related to Internet fraud, works to quantify fraud patterns, and provides timely statistical data of current fraud trends.[117]

Furthermore, in order to ensure international cooperation in the cyber-crime domain, a cyber-crime fighting service was created as an online contact centre available permanently on this website, where FBI statistics from the Internet Crime Complaint Center are posted.

According to the 2007 Internet Crime Complaint Centre, Canada was ranked number 4 with 5.6%, and Romania was ranked number 5 with 1.5% in the list of the top ten countries in terms of the number of cyber criminals.[118] Interestingly, in 2008, Canada was still ranked number 4 with 3.1 %, while Romania was ranked number 10 with 0.5%.[119] Romania's latest ranking means that Romania's cybercrime activity decreased during 2007. The Internet Crime Complaint Center compiles its statistics about criminal activity, criminal devices, fraudulent schemes, and types of cyber offenders (e.g., fraudsters) from the reports of complainants. As well, the Center identifies a perpetrator's characteristics in terms of gender, age, geographical residence, and relation to the complainants, the average loss per typical complainant, etc.

---

[116] Statistics Canada. *Population Estimate (January 2009)* 13 May 2009 < http://www.statcan.gc.ca/daily-quotidien/090326/dq090326a-eng.htm>.

[117] Ministry of Communications and Information Technology, www.efrauda.ro 10 May 2009 http://www.efrauda.ro/efrauda/admin/default.aspx?StartTab=0&lang=2.

[118] The Internet Crime Complaint Center (IC3) began its activity activity in 2000 as a partnership between the National White Collar Crime Center (NW3C) and the Federal Bureau of Investigation (FBI). Internet Crime Complaint Center, *2007 Internet Crime Report.* 20 Dec. 2008 < http://www.ic3.gov/media/annualreports.aspx> 9, Map 2. This report contains a useful appendix with an explanation of complaint terms (i.e. insurance fraud, identity theft, confidence fraud, Nigerian letter fraud etc.) and the best practices to prevent fraud (i.e., prevention tips).

[119] Internet Crime Complaint Center, *2008 Internet Crime Report* 4 April 2009 <http://www.ic3.gov/media/annualreports.aspx> 7, Map 2.

The number of cyber offences seems to be large for Romania. For example, in 2005, the Minister of Communications and Information Technology (M of F C and IT), Zsolt Nagy, participated in the "Electronic Communications and IT" seminar organized in the Campaign for the Preparation of the Business Community in Romania for the EU accession at the headquarters of the Chamber of Commerce and Industry of Romania. He declared:

> Last year, the specialized services in Romania examined 579 informational offences out of which 237 represent Internet frauds, 114 informational offences, 103 credit card offences, 30 cases of infantile pornography and 95 other informational offences. The number of arrested persons for these offences is 345 and 46 of those were charged. The positive aspect is that, although the number of Internet users has grown up to 28% of the population in 2005, Romania's ranking in the list of the top countries in terms of cybercrime continues to decline.[120]

According to the M of F C and IT, "In 2005, for the offences regarding Internet frauds, 149 persons have been arrested out of which 13 were charged; for the informational offences, 76 persons have been arrested and 4 charged; the number of persons arrested for credit card offences was 68, out of which 23 were charged. For child pornography, 31 persons have been arrested and 2 charged, and for other informational offences, 21 persons have been arrested and 2 charged."[121]

The level of corruption in both countries differs and can be related to cybercrime. For instance, Transparency International rates 180 countries according to level of corruption, with number 1 on the list indicating "Least Corrupt."[122] In 2008, Canada occupied number 9 on this

---

[120] Ministry of Communications and Information Technology, *Ensuring the Security of the Information Systems, Priority of MCTI* 3 March 2006, 12 May 2009 http://www.efrauda.ro/efrauda/admin/default.aspx?StartTab=0&lang=2>.

[121] Ministry of Communications and Information Technology, *Ensuring the Security of the Information Systems, Priority of MCTI.*

[122] Transparency International. *Corruption Perceptions Index 2008* 20 April 2009 < http://www.transparency.org/policy_research/surveys_indices/cpi/200>.

global corruption perception index, and Romania was assigned number 70. It seems that a more corrupt state generates more cybercrime than a less corrupt state (traditional criminal activity is also more evident in a corrupt state than in a less corrupt one). As we have seen, Romania's ranking in relation to cybercrime complaints, according to the Internet Crime Complaint Center, went from number 4 to number 10 in 2007/2008 while Canada's ranking remained unchanged. This difference does not imply that Romania's corruption decreased more than Canada's in 2008 compared to 2007, but simply that the number of complaints does not correspond exactly with the actual number of Romanian criminals (as we can imagine, their criminal activities are becoming more refined and more difficult to detect), or that the statistics are not very sophisticated in terms of criteria (i.e., accounting for the diversity and diversification of cybercrimes).

A specific Internet crime in both countries can be compared to see the differences in offender methodology, for example auction fraud which led to one of the most common complaints in 2008. Auction fraud occurs when someone (usually a private individual, male, between the ages of 30 to 50) advertises items for sale such as: electronics, game consoles, smart phones, and even very cheap merchandise such as stuffed animals (e.g. teddy bears). Usually, the victim is asked to pay through wire transfer, money order, Western Union, etc. Of course, the merchandise is never received by the buyer, and the offender's address is usually a mailbox or a post office. This fraud is doable because the buyers will not hesitate about sending money if the amount is not too high, or if the product is priced much lower than the regular price.

Auction fraud provides an example of another difference between Canada and Romania in terms of mentality, background and e-commerce history. According to the statistics listed in the 2008 Internet Crime Complaint Center (IC3) Report, Canada is ranked number 4 in the world in terms of cyber criminals, as discussed previously, and number 2 in terms of victims. In the same

report, Romania is ranked number 10 in terms of criminals and is not even listed among the top 10 countries in terms of victims. In Canada, a relatively large proportion of the population is used to and educated about e-commerce. Canadians regularly participate in it, are comfortable with online transactions, and have greater access to the Internet than people do in Romania. Democracy, the free market, and the e-commerce mentality cause Canadians to become innocent victims in Internet fraud schemes. Romania is not even included in this top 10 list of victims because Romanians do much less e-commerce and online transactions, but despite this, Romania is in the Top 10 cybercrime offenders.

For example, auction fraud is more difficult to commit for Romanians than for Canadians because Romanians need to have an excellent command of the English language (which is not their mother tongue). Otherwise, the victims will become suspicious of a seller who claims that he is located in Texas, for example, but speaks poor English. Also, setting up a P.O. box in the US or Canada is much harder for Romanians than Canadians because Romanians are overseas and they need to have an accomplice in North America in order to receive the money because very few buyers will send it directly to Romania. Canadians appear to be able to commit auction fraud more easily than Romanians can; however both Canada and Romania are ranked very closely in the list of the top 10 countries for Internet Fraud, according to the IC3. Two countries will not differ greatly in the fight against cybercrime if one country (i.e., Romania) accepts international conventions or close surveillance of the Internet but does not always apply it in practice and another country (i.e., Canada) does not apply the Conventions' legislation. The Convention on Cybercrime might not be effective, yet Romania, which follows the Convention, and Canada, which does not, are still both included in the list of the top 10 countries for Internet fraud. This Thesis questions how an international convention can be applied universally to

different countries with significant differences in mentality, economies, and Internet accessibility and utilization. Perhaps the Convention on Cybercrime is not being ratified according to the specific needs of a country but instead is being ratified for political or regional reasons, and since Canada is number 2 in the list of the top 10 countries in terms of cyber fraud it should be more concerned than Romania about fighting Internet crime and should, logically, ratify the Convention on Cybercrime (which, at least in theory, would help Canada in its fight against cybercrime). In contrast, Romania, which is not even included in the above mentioned list and has already signed and ratified the Convention, does not need to fight against this form of cybercrime as much as Canada does, accordingly to the statistics.

A comparison of the demographics in each country might also indicate a direction for cybercrime investigation.[123] Canada's population in January 2009 was about thirty-six million citizens; Romania's population in January 2009 was about twenty-one million[124] within a total geographical area that is forty-one times smaller than Canada's.[125] In a small country like Romania, which has a high level of corruption and a precarious economy, cybercriminal activity will be closely linked to these factors. Thus, financial fraud is a frequent type of cybercrime in

---

[123] I acknowledge that Dr. Paul Youngman (University of North Carolina - Charlotte) suggested that I should look at the population of each country. Dr. Youngman made this suggestion on the occasion of a presentation that I delivered at an international conference dedicated to current graduate research in humanities computing. My paper entitled "Regulation of Cybercrime in a Global Village" was a preview of my master's thesis and was delivered at the *Beyond Analogue* conference, University of Alberta, Humanities Computing Programme, February 13, 2009.

[124] Romania. National Institute of Statistics, *Populatia Stabila la 1 Ianuarie 2009* (*Stable Population at 1 January 2009)* 13 May 2009 http://www.insse.ro/cms/rw/pages/index.ro.do.

[125] Romania's total geographical area is 238 391 km^2 and Canada's is 9 984 670 $km.^2$ For the geographical data, see the Government of Canada's website (http://canada.gc.ca/home.html) and Romania's website (www.gov.ro).

Romania, as was shown in Chapter Three. In Canada, cybercrime is related to its low level of corruption and its well-developed economy. In this case, the cyber offences are much more diversified than economic computer-related offences and include mischief in relation to data, the exposure of children to inappropriate material including child pornography, violence and hate websites, threatening email, and personal information made public.[126]

The complexity of regulating cybercrime globally has been shown through the examples of Canada and Romania, which have two different "democracies" and different cultures, technologies, and economies. Geography and human behaviour are important factors in the struggle against cybercrime. The relationships among democracy, technology, and government cybercrime regulation within the world are problematic. Each democracy has its own limitations, as does the Convention on Cybercrime as a model. Stronger and more powerful ways are needed to develop local strategies that can be combined with the global recommendations of the Convention on Cybercrime, which stipulates that: "Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to search or similarly access ..."[127] Canada and Romania, two democracies, have to consider their different histories and different public policies when adopting the same international conventions.

---

[126] Kowalski 15-17.

[127] Council of Europe. Convention on Cybercrime CETS no 185 23 November 2001. 18 September 2008 <http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=185&CM=8&DF=9/5/2007&CL=ENG>.

Conclusion

This Thesis analyzed the global Convention on Cybercrime in relation to the perceptions of cybercrime and Internet regulation within Canada and Romania. Both countries signed the Convention on Cybercrime on 23 November 2001. Although Canada did not ratify it, Romania ratified the Convention, which came into effect on 12 May 2004.

This Thesis examined the many differences between Canadian and Romanian democracies, economies, cultures, infrastructures, legal systems, and cyber offences, which showed that Internet regulation on a national level is more practical than a global regulatory model (the Convention on Cybercrime). It was also shown that technological development (i.e., Internet technology), the transnational character of computer-related crimes, and the global accessibility to the global information society make the Convention ineffective.

Chapter One covered the historical roots, explanatory reports, and debates regarding the content and aims of the Convention on Cybercrime, which was discussed because the Internet and cybercrime is a global issue and has unique characteristics. Because of the global and borderless nature of the Internet and Cybercrime, the Convention was drafted by multiple EU and non-EU countries. This Convention was signed and ratified by some EU and non-EU countries because the notion of a "treaty" within a global world is not applicable to every country (e.g., Canada). The content and computer-crime terminology used in the Convention on Cybercrime were examined in order to identify the features of cybercrime and the actors involved in it (e.g., the typology of cybercrimes, the offenders, and the use of the computer as a tool). It was shown that cybercrime, which is borderless and involves transnational offenders, has no clear definition. The model of Internet regulation proposed by the European Convention on Cybercrime has a problematic relationship with each state's collective regulations and economic and political

organizations, and each citizen's individual self-regulation. As a result, the international community should try to accommodate the national differences based on the specific culture and notion of democracy of each national state. Other differences are in terms of safety, equality and electronic media usability. In addition to the Convention on Cybercrime, other controversial international treaties have been difficult to implement globally due to differences in local legislation and cultures (e. g., "human rights," and "women's rights" treaties).

Chapter Two discussed Canada's modern and strong democracy – its political and economic system governed by neo-liberal public policy. Some scholars have studied the relationship between economic rights and democratic rights, concluding that Canadian policy makers' decreasing concern with the public interest demonstrates the limitations of neo-liberal policy in relation to the Internet. However, the Canadian government has undertaken initiatives to regulate the Internet. Some scholars recommend the ratification of the Convention on Cybercrime by the Canadian government in order to fight internationally against specific Internet crimes (e.g., child pornography). Doing so would involve harmonizing the ISPs for data transmission even though this Convention's stipulations are against the interests of private users. Such an action could lead to ethical problems. According to the Centre for Democracy and Technology and Canadian Centre for Justice Statistics, Canada has advanced technology (which gives the citizens the opportunity to have easy access to political institutions) as well as a high crime rate. Above all, some Canadian governmental representatives have criticized Canada's slow action on cybercrime. Technology and legal jurisdiction are importance because some technical problems must be solved in order for the Canadian police to retain online data. Canada recognizes that contemporary Internet-based offences are a major problem. Canada has a developed Global Information Society (GIS), a strong democracy, and multiculturalism. Still, Canada signed the

Convention on Cybercrime but did not ratify it, because Canada has some issues regarding the harmonization of human rights and federal legislation against cybercrime.

In Chapter Three, Romania's new capitalist system and its fragile democracy was examined in relation to the Convention on Cybercrime. The Romanian democracy has a recent history of just twenty years after almost fifty years of a communist totalitarian system. The Romanian political and economic systems are governed by a market-based public policy. Some Romanian scholars have studied the relationship between democracy and the implementation of cybercrime legislation with help from international institutions due to Romania's previous political and economical system. Ethical issues exist at the global level (e.g., a Romanian NASA hacker was wanted by IBM), and privacy issues are important to Romanians within a society recovering from almost fifty years of totalitarian surveillance. According to the Center for Democracy and Technology, Romania has basic technology and a high crime rate. In order to prevent and fight against computer-related crime, the Romanian state signed the Convention on Cybercrime on 23 November 2001 and adopted Law 161/2003 to harmonize Romania's national legislation with the provisions stipulated in the Convention. Later on 12 May 2004, Romania ratified the Convention, having already incorporated its provisions into the local legislative framework. Romania used the Convention as a guideline when implementing the Convention's articles one by one. Therefore, the Romanian cybercrime legislation is compatible with international standards, defines cybercrime terminology (computer-system, computer data, service provider, traffic data, child pornography, data on the users/subscriber information) as the Convention stipulates, and offers additional information on how to fight cybercrime (e.g., on automatic data processing and computer program). As well, Romania, which recently became part of the EU, has an undeveloped Global Information Society (GIS) and a weak democracy and

national ideology. Romania signed and ratified the Convention on Cybercrime, but cybercrime is common within a public structure where both state Internet regulation and citizens' self-regulation are weak, and financial fraud is likely to occur due to the unstable economy.

Chapter Four examined how the Convention on Cybercrime is being implemented in Canada and Romania and how the global model of Internet regulation is being applied regionally. The more technology a country develops, the more that country seems to experience cybercrime and cyber threats against ordinary Internet users. Technology comes as a package; it not only benefits but also harms individuals and social structures. Furthermore, the Convention on Cybercrime seems to involve a paradox. The goal of the Convention was to follow the European Convention on Human Rights, Freedoms and the Right to Privacy, but the principles expressed in the same Convention seem to violate human rights and the right to free expression by advocating preserving and retaining the personal data of free individuals.

Canada's and Romania's extradition treaties are interesting subjects to address in relation to cybercrime because both of them have these treaties in place, but Romania refused to extradite the Romanian hacker Vlad Duiculescu. Moreover, both countries have a different level of corruption and this can be related to cybercrime. Finally, in 2008, auction fraud was one of the most commonly reported cybercrimes. Auction fraud appears to be easier to commit in Canada than in Romania, but both countries are ranked very closely in the list of the top 10 countries for Internet fraud, accordingly to IC3. Even if one country (i.e., Romania) implements the Convention on Cybercrime and close surveillance, and another country (i.e., Canada) does not apply the Convention's legislation and close surveillance, the two countries will not differ greatly in combating or fighting against cybercrime, which shows the ineffectiveness of the Convention. The complexity of regulating cybercrime is demonstrated by the examples of Canada and

Romania, which have two different “democracies” and different local cultures, technologies and economies. Geography and local behaviour are important when fighting against cybercrime, because of their unique nature. The relationships among democracy, technology, and government cybercrime regulation within a global world are problematic.

It was shown that the Council of Europe with its Convention on Cybercrime has claimed that one form of global Internet regulation is appropriate for all countries. In contrast, I argued that the structural, legal, economic, and socio-cultural aspects of local cultures affect the global homogenous regulation of the Internet. The relationship between a global model of Internet regulation (i.e., Convention on Cybercrime) and its individual implementation in specific countries and specific legal frameworks (e.g., legislation concerning consumer privacy or human rights) is problematic.

The Convention on Cybercrime as a tool in the global fight against computer-related offences is far from perfect and has not proved to be globally effective; yet, the Convention does represent a good serious effort. National ratifications of the Convention rely on local legislation, and so the entire structure has the virtue of being able to improve by learning from practice (different democracies, different technological development, different rules regarding private users, their rights, interest and privacy, and freedom of speech). Improvement of this kind require a long time and meticulous attention in order to be adjusted to specific socio-economic cultures and national legal frameworks.

In addition to improvements relating to the way the Convention is implemented, the actual Convention on Cybercrime also needs to be refined and improved. The Convention might rightly be considered an ongoing experiment, since the rule-making process is an on-going one. The Convention recommendations should be taken into consideration and used as guidelines until

a smooth transition can be made from this guideline status to a more robust version that deals more clearly with issues of enforcement. Producing such a revision will require an international effort of all the countries involved in this process. It is always better to have regulations in place, even if they are experimental ones. Throughout the process, the Council of Europe should offer instructional sessions to the Countries that have already adopted the Convention and applied its regulations. For example, Romania intercepts and stores all phone calls and online traffic data, claiming that this is stipulated by the Convention recommendations, but is this actually the intention of the Convention? A series of instructional sessions might help to clarify such contentious points.

One of the main concerns raised by Peng (2009) – when discussing internet regulation within different Western and non-Western cultures – addresses the value of regulation and the mechanism of regulation. He talks about the five steps of Internet supervision where specific actors are involved in cyber regulation, ranging from the government policy makers to the government regulators. The mechanism of regulation ranges from self-regulation with self-sanction to legal regulation with state enforcement and coercive sanctions (even if the governments are aware that the regulation of the internet is limited and many internet actors are transnational). The first internet regulator is the individual who approaches the internet with his/her own personal ethics (this is a personal mechanism implying self-sanction). Then we have the second party (i.e., the person acted upon) who can apply filter software and other technology in order to fight against cyber crime. In support of this second group, there should be constant public campaigns and seminars organized by NGOs and public bodies in order to make internet users aware of cybercrime and methods available to prevent and fight against it. Third, we have non-hierarchically organized social forces and hierarchically organized non-governmental

organizations that can help regulate the internet. For instance, the internet providers should be responsible for the internet content based on some code of conduct and industry self-regulation.

In Canada, change has come slowly. As Peng has observed, internet regulation is a dynamic procedure requiring constant learning, updating and global dedication. Nine years have passed since the Convention was drafted and signed; yet, there have only been small steps taken to ratify and apply it to local legal frameworks that are in any case developing slower than internet technology and the expertise of cyber offenders. The Canadian government – the last regulatory body according to Peng's mechanism of regulation framework – should take the rapid advances in technology and offender expertise into consideration when deciding to ratify and implement the newest version of the Convention on Cybercrime. In addition to governmental regulation of internet activities (which is an ongoing process because the internet technology is developing) there is a need for self-regulation that would be promoted by public campaigns. As well, the Convention recommendations should be transposed into Canadian federal law, acknowledging that the greater good, democratic rights and the rights to a safe life should supercede some economic rights and contextual situations (i.e. those of Internet Service Providers). Personal ethics, local social norms, public laws and self-regulation by industry should all be taken into consideration by the Canadian government when accommodating the Convention on Cybercrime guidelines.

The Canadian government as a national regulator might be a path opener, an internet regulation pioneer, and it should consider proposing some alterations to the Convention on Cybercrime before considering ratifying and implementing the Convention as it is. It might, for instance, think to catch up with technology and security issues by proposing "an internet passport" as an effective quality tool for fighting against cybercrime. Internet users would

identify themselves online using their internet passports, in a manner that is intended to be safer than the current IP addresses, which are easy to hide and are in any case not necessarily associated with individual users.

Furthermore, having international cybercrime guidelines is needed, but international law may be more useful in some areas. For instance, child pornography is a terrible cybercrime, and is explained and condemned within the Convention on Cybercrime. However, it should also be possible to establish an international law on child pornography, stipulating the same international punishments for the same crimes no matter the country. As such, cyber offenders might be judged globally.

Other research topics related to cybercrime include: the notion of state overregulation and its relationship with self-regulation in different socio-political structures; online information ownership; cyber-privacy as it occurs in different public and private spaces (e.g., Canada and Romania).The study of these research topics would add new layers of complexity to the analysis of the Convention of Cybercrime in the context of the multifaceted and global cyber criminal activities and would assist in developing real solutions for fighting and preventing cybercrime.

Bibliography

Abbate, Janet. "From ARPANET to Internet." *Inventing the Internet*. Cambridge: MIT Press, 1999. 113-146.

---. "Government, Business and the Making of the Internet" *Business History Review* 75.1 (2001): 147-176.

AFP, "Romania - a Country that Fights against Cybercrime," 24 November 2008, 6 January 2009 <http://www.euractiv.ro/uniunea-europeana/articles%7CdisplayArticle/articleID_15579/AFP-Romania-o-tara-care-se-lupta-cu-criminalitatea-informatica.html

American Society of International Law. *ASIL Guide to Electronic Resources for International Law* 5 April 2009 < http://www.asil.org/treaty1.cfm>

Amza, Tudor and Cosmin-Petronel Amza. *Criminalitatea Informatica (Cybercrime).* Bucuresti: Lumina Lex Publishing House, 2003.

APTI. "Justitie in Era Digitala (Justice in Digital Era)," agenda (Timisoara, Romania, 4-5 December 2008), 10 May 2009 < www.apti.ro/webfm_send/19>

Axworthy, Thomas, Leslie Campbell and David Donovan. *The Democracy Canada Institute: a Blueprint*. Montreal, Quebec: Institute for Research on Public Policy = Institut de Recherche en Politiques Publiques, 2005 Gibson Library Connections, 2008.

Barber, Benjamin. *Strong Democracy: Participatory Politics for a New Age.* 20th ed. Berkeley: University of California Press, 2003.

Basedow, Jürgen and Toshivuki Kono, ed. *Legal Aspects of Globalization: Conflict of Laws, Internet, Capital Markets, and Insolvency in a Global Economy.* The Hague; Boston: Kluwer Law International, 2000.

Campbell, Dennis and Chrysta Ban, eds. *Legal Issues in the Global Information Society.* New York: Oceana Publications, 2005.

Caudill, Eve M. and Patrick E. Murphy. "*Consumer Online Privacy: Legal and Ethical Issues*." *Journal of Public Policy & Marketing* 19.1 (2000): 7-19.

Chu, Showwei. "Canada Lags in Cybercrime Laws." *Technology Reporter* 14 Dec. 2000. 13 Jan. 2009. <http://www.infosecnews.org/hypermail/0012/3233.html

Clyburn, Lisa Dawn." Internet Crimes: Can and Should the Internet be Regulated?" M.Ed. Thesis University of Alberta, 1998.

---. *Convention on the Elimination of All Forms of Discrimination against Women: Reference Document*. Ottawa: Dept. of the Secretary of State, 1986.

Council of Europe. *Convention on Cybercrime CETS no 185, 23 November 2001*. 18 September 2008 <http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=185&CM=8&DF=9/5/2007&CL=ENG>.

- - -. *Convention on Cybercrime: Explanatory Report. ETS no 185.* 14 November 2001. 3 Jan. 2009 <http://conventions.coe.int>

- - -. *The Council of Europe and Cybercrime. Factsheets updated 24 November 2008*. 1 April < http://www.coe.int/t/dc/files/themes/cybercrime/default_en.asp>

- - -.Global Reach of the Council of Europe Convention of Cybercrime (as of 9th March 2009). 2 April 2009 https://wcd.coe.int/ViewDoc.jsp?id=1414219&Site=DC&BackColorInternet=F5CA75&BackColorIntranet=F5CA75&BackColorLogged=A9BACE

- --. *Additional Protocol to the Convention on cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems CETS No.: 189*. 27 March 2009 <http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=189&CM=8&DF=17/02/2006&CL=ENG>.

Craiutu, Aurelian. "*Romania: The Difficult Apprenticeship of Liberty (1989-2004),*" *East European Studies* lectures, Meeting Report 298, 9 June 2004, Woodrow Wilson International Center for Scholars, 3 Jan. 2009 <http://www.wilsoncenter.org/index.cfm?topic_id=1422&fuseaction=topics.publications&doc_id=96456&group_id=7427>

" The CRTC Examines Internet Regulation and Issues in Canada," 14 August 1998, 4 January 2009 <http://canadaonline.about.com/library/weekly/aa081498.htm>.

"Canadian Government Will not Try to Regulate the Internet," 22 May 1999, 4 January 2009 <http://canadaonline.about.com/library/weekly/aa052299.htm>.

Cyber Tribunal. 20 April 2009 http://www.cybertribunal.org/index.en.html

"Cybercrime," *Market Watch* 8 September 2004, 6 January 2009 <http://www.marketwatch.ro/articol/263/Criminalitatea_informatica/>

Ding, Julian. "Internet Regulation." *Legal Issues in the Global Information Society.* Eds. Dennis Campbel and Chrysta Ban. New York: Oceana Publications, 2005. 279-351.

Duhaime, Lloyd. "Extradition from Canada," 2 May 2009 <http://www.duhaime.org/LegalResources/CriminalLaw/LawArticle-99/Extradition-Law-Canada.aspx>

European Commission. *Treaties Office Database* 5 April 2009 < http://ec.europa.eu/world/agreements/glossary/glossary.jsp?internal=true>

Flores, Arturo Azuara. "To Each Country, its Own Law and Domain: the Legal Structures of ccTLD's in Comparative Perspective." Diss. Tulane University, 2008.

Forsey, Eugene. *How Canadians Govern Themselves.*6th ed. Ottawa: Library of Parliament, Public Information Office, 2005.

Froomkin, Michael. "The Death of Privacy?." *Stanford Law Review* 52.5 (2000): 1461-1543.

Georgescu, Ionel. "Infractiunile Informatice Prevazute de Legea Nr. 161/2003 (Cybercrimes according to the Law 16/2003)," *Buletin Documentar* 3 (2005) 7 pp. 3 January 2009 <http://www.pna.ro/text_doctrina.jsp?id=46>

Gerlach, Natascha. "Regulating the Internet: A Futile Effort? The Case of Privacy in a German-Canadian Comparative Study." L.L.M. thesis Queen's University at Kingston, 1999.

Goldsmith, Jack L. *Who Controls the Internet?: Illusions of a Borderless World.* New York: Oxford University Press, 2006.

Harvey, Pierre-Léonard. *La Démocratie Occulte: Rapports de Force, Gouvernance et Communautique dans la Société de l'Information.* Québec : Presses de l'Université Laval, 2004.

Iliescu, Ion. *Communism, Post-Communism and Democracy: the Great Shock at the End of a Short Century*. Interviewed by VladimirTismaneanu. Boulder: East European Monographs; New York: Columbia University Press, 2006.

Internet Crime Complaint Center. *2007 Internet Crime Report.* 20 Dec. 2008 < http://www.ic3.gov/media/annualreports.aspx>

---.*2008 Internet Crime Report*. 4 April 2009 http://www.ic3.gov/media/annualreports.aspx

Jurkowski, Diane and George Eaton, eds., *Between Public and Private: Readings and Cases on Canada's Mixed Economy*. Concord, Ont: Captus Press, 2003.

Kowalski, Melanie. *Cyber-Crime: Issues, Data Sources, and Feasibility of Collecting Police-Reported Statistics***.** Ottawa: Canadian Centre for Justice Statistics, 2002.

Kunz, Jean. *From Mosaic to Harmony: Multicultural Canada in the 21st century: Results of Regional Roundtables*, Ottawa, Ont.: Policy Research Initiative, 2007 Gibson Library Connections, 2008.

LaSelva, Samuel. *The Moral Foundations of Canadian Federalism: Paradoxes, Achievements, and Tragedies of Nationhood.* Montreal, Québec: McGill-Queen's University Press, 1996.

Levine, Andrew. *Political Keywords: A Guide for Students, Activists, and Everyone Else.* Malden, MA: Blackwell Publishing, 2007.

Lessig, Lawrence. *Code and Other Laws of Cyberspace.* New York: Basic Books, 1999.

Malecki, Edward. "The Economic Geography of the Internet's Infrastructure." *Economic Geography* 78.4 (2002): 399-424.

Marsden, Christopher, ed. *Regulating the Global Information Society.* Warwick Studies in Globalisation. London; NewYork: Routledge, 2000.

McNutt, Kathleen and Meaghan Carey. *Canadian Digital Government***.** Regina, Sask.: Saskatchewan Institute of Public Policy, Gibson Library Connections, 2008.

Mixich, Vlad. "How Much is Your Personal Data?," *Hotnews*, 22 January 2009 <http://www.hotnews.ro/stiri-opinii-5343895-cat-costa-datele-tale-personale.htm>

Murray, Andrew D**.** *The Regulation of Cyberspace: Control in the Online Environment.* Abingdon: Routledge-Cavendish, 2007.

Peng, Hwa Ang. *Ordering Chaos: Regulating the Internet*. Singapore: Thomson Learning, 2005.

-- -. How Countries Are Regulating the Internet Content. 20 Jan. 2009 <http://www.isoc.org/inet97/proceedings/B1/B1_3.HTM#s11>

Prompt Media, "Bucuresti: Certificat European privind Criminalitatea Informatica si Probele Electronice pentru Judecatorii, Procurorii si Avocatii Romani, " 6 January 2009 <http://www.promptmedia.ro/stiri/1-stiri/7545-bucuresti-certificat-european-privind-criminalitatea-informatica-si-probele-electronice-pentru-judecatorii-procurorii-si-avocatii-romani->

Reddick, Andrew James." The Duality of the Public Interest: Networks, Policy and People." Diss. Carleton University, 2002.

Reidenberg, Joel R. "Resolving Conflicting International Data Privacy Rules in Cyberspace." *Stanford Law Review* 52.5 (2000): 1315-1371.

---." Technology and Internet Jurisdiction." *University of Pennsylvania Law Review* 153.6 (2005): 1951-1974.

Robertson, David. *The Routledge Dictionary of Politics*, 3rd ed. London: Routledge, 2004.

Romania. Ministerul Comunicatiilor si Tehnologiei Informatiei (Ministry of Communications and Information Technology). *Ghidul pentru Aplicarea Dispozitiilor Legale referitoare la Criminalitatea Informatica* (*Handbook for the Enforcement of Legal Provisions Regarding Informatics Crime*). US Embassy in Bucharest, USAID and RITI, 2004. 6 January 2009 <http://www.mcti.ro/index.php?id=28&lege=813&L=0>

-- -. Autoritatea Nationala de Supraveghere a Prelucrarii Datelor cu Caracter Personal (The National Supervisory Authority for Personal Data Processing). Directive 2006/24/EC Of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC. 27 Jan. 2009 http://www.dataprotection.ro/index.jsp?page=legislatie_comunitara&lang=en

- --. National Institute of Statistics, *Populatia Stabila la 1 Ianuarie 2009* (*Stable Population at 1 January 2009)* 13 May 2009 http://www.insse.ro/cms/rw/pages/index.ro.do

Romania. Ministry of Foreign Affairs of, *Remarks at the Signing Ceremony for the Protocols of Exchange of Instruments of Ratification for the US-Romania Mutual Legal Assistance Protocol and the US-Romania Extradition Treaty* 12 May 2009 < http://www.mae.ro/index.php?unde=doc&id=13446>

Saco, Diana. *Cybering Democracy: Public Space and the Internet.* Minneapolis: University of Minnesota Press, 2002.

Satapathy, C. "Role of the State in the E-World." *Economic and Political Weekly* 35.39 (2000): 3493-3497.

Schulman, Cristina. “The Implementation of the Convention on Cybercrime in Romania,” handout, Workshop on Cybercrime for Hon. Judges and Workshop for Investigators, Prosecutors and Lawyers (Colombo, Sri Lanka, 27-28 October 2008), 7 January 2009 <www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/cy_activity.../567-IF08-CRISTINA_SCHULMAN_HandOut.PDF>

Showwei, Chu. “Canada is a Laggard in Enacting Laws to Crack Down on Cybercrimes,” *Globe and Mail* 14 December 2000. 23 January 2009 <http://www.infosecnews.org/hypermail/0012/3233.html>

Seger, Alexander. “The Convention on Cybercrime of the Council of Europe.” 2nd WSIS Action Line C5, Geneva, 14-15 May 2007. 20 Jan. 2009 <www.coe.int/economiccrime>

---. “Cybercrime Legislation - Country Profile – Romania,” April 2008, COE, 2 May 2009 <http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Country Profiles/default_en.asp>

Shaw, Gillian. “Canada 'Reputed to be Lax on Cybercrime'.“ *Times Colonist* 25 November 2008. 20 Jan. 2009 <http://www.timescolonist.com/news/Canada+reputed+cybercrime/991226/story.html>

Smihily, Maria. *Internet Usage 2007, Household and Individuals*, Eurostat, 7 May 2009 < http://epp.eurostat.ec.europa.eu/cache/ITY_OFFPUB/KS-QA-07-023/EN/KS-QA-07-023-EN.PDF>

Smyth, Sara M. “Child Pornography on the Internet: An International "Crisis" from a Canadian Perspective.” Diss. York University (Canada), 2008.

Statistics Canada. *Canada’s Journey to an Information Society* Catalogue no. 56-508-XIE 2003, 5 April 2009 <ht*p://www.statcan.gc.ca/bsolc/olc-cel/olc-cel?lang=eng &catno=56-508-X*>

---. *Population Estimate (January 2009)* 13 May 2009 < http://www.statcan.gc.ca/daily-quotidien/090326/dq090326a-eng.htm>

Transparency International.*Corruption Perceptions Index 2008.* 13 April 2009 <http://www.transparency.org/policy_research/surveys_indices/cpi/2008>

United Nations Interregional Crime and Justice Research Institute (UNICRI). “Cybercrimes - HPP,” 3 May 2009 http://www.unicri.it/wwd/cyber_crime/hpp.php

---. “European Certificate on Cybercrime and Electronic Evidence,” 3 May 2009 < http://www.unicri.it/wwd/cyber_crime/ecce.php>

Vasiu, Ioana and Lucian Vasiu. *Prevenirea Criminalitatii Informationale (Cybercrime Prevention).* Bucuresti: Hamangiu Publishing House, 2006.

Verdery, Katherine. *National Ideology under Socialism: Identity and Cultural Politics in Ceausescu's Romania*. Berkeley: University of California Press, 1991.

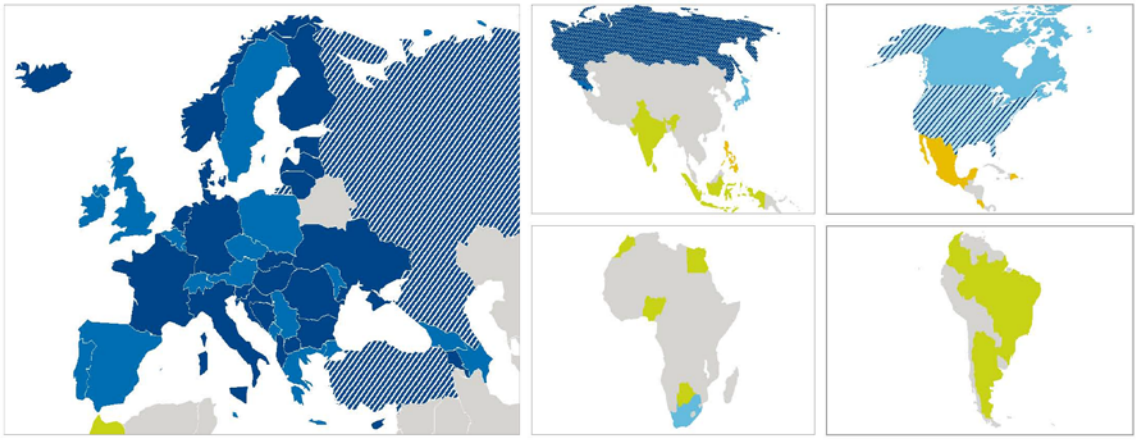
Warf, Barney and John Grimes. “Counterhegemonic Discourses and the Internet.” *Geographical Review* 2.87 (1997): 259-274.

Yakovlev, Alexander ed., *The Yalta Conference, 1945: Lessons of History* (Moscow: Novosti Press Agency Pub. House, 1985).

Appendix 1

This map was made public on the occasion of the conference **"**Criminalising Child Pornography, Training, Tracking Money on the Internet: Programme Features of the 2009 Council of Europe Conference on Cybercrime" hold in Strasbourg on 9-10 March 2009. 2 April 2009. https://wcd.coe.int/ViewDoc.jsp?id=1414219&Site=DC&BackColorInternet=F5CA75&BackColorIntranet=F5CA75&BackColorLogged=A9BACE

Global reach of the Council of Europe Convention on Cybercrime



Countries party to the Convention

Council of Europe member states

Albania, Armenia, Bosnia and Herzegovina, Bulgaria, Croatia, Cyprus, Denmark, Estonia, Finland, France, Germany, Hungary, Iceland, Italy, Latvia, Lithuania, Netherlands, Norway, Romania, Slovak Republic, Slovenia, «the former Yugoslav Republic of Macedonia », Ukraine

Non Council of Europe member states

United States*

Signatory countries

Council of Europe member states

Austria, Azerbaijan, Belgium, Czech Republic, Georgia, Greece, Ireland, Liechtenstein, Luxembourg, Malta, Moldova, Montenegro, Poland, Portugal, Serbia, Spain, Sweden, Switzerland, United Kingdom

Non Council of Europe member states

South Africa, Canada*, Japan*

Countries which did neither ratify nor sign the Convention

Council of Europe member states

Andorra, Monaco, Russia, San Marino, Turkey

Source: Council of Europe, 9th March 2009

Countries that are known to use the Convention as a guideline for their national legislation

Non Council of Europe member states

Argentina, Botswana, Brazil, Colombia, Egypt, India, Indonesia, Morocco, Nigeria, Sri Lanka

Non Council of Europe member states invited to accede

Costa Rica, Dominican Republic, Mexico*, Philippines

* observer countries

Appendix 2

Project on Cybercrime
www.coe.int/cybercrime

COUNCIL OF EUROPE CONSEIL DE L'EUROPE

Version April 2008

Cybercrime legislation – country profile

ROMANIA

This profile has been prepared within the framework of the Council of Europe's Project on Cybercrime in view of sharing information on cybercrime legislation and assessing the current state of implementation of the Convention on Cybercrime under national legislation. It does not necessarily reflect official positions of the country covered or of the Council of Europe.

Alexander Seger
Economic Crime Division
Directorate General of Human Rights and Legal Affairs
Council of Europe, Strasbourg, France
Tel: +33-3-9021-4506
Fax: +33-3-9021-5650
Email: alexander.seger@coe.int
www.coe.int/cybercrime

Country:	**Romania**
Signature of Convention:	Yes: 23.11.2001
Ratification/accession:	Yes: 12.05.2004
Provisions of the Convention	***Corresponding provisions/solutions in national legislation*** *(pls quote or summarise briefly; pls attach relevant extracts as an appendix)*
Chapter I – Use of terms	
Article 1 – "Computer system", "computer data", "service provider", "traffic data	ART. 35 of Romania Law no 161/2003 All the terms required by the Convention to be defined "computer system", "computer data", "service provider" and "traffic data" (article 1), "child pornography" (article 9) and "subscriber information" (article 18) are covered by Art. 35 of Law no 161/2003. Romanian Law provides also for some additional definitions: • *automatic data processing* • *computer program* • *security measures* • *without right* **General remark regarding the mental element.** Under the Romanian legal system ***an act that resides in an action committed with negligence shall be an offence only when the law provides this expressly*** (article 19 paragraphs 2 Criminal Code). As a result of this provision it was stated that there is no need to specify expressly the intentional element in the text. If the law **does not provide any mental element in the case of an offence consisting of an action the mental element required is**

	intend.
Chapter II – Measures to be taken at the national level *Section 1 – Substantive criminal law*	
Article 2 – Illegal access	ART.42 of Romania Law no 161/2003
Article 3 – Illegal interception	ART.43 of Romania Law no 161/2003
Article 4 – Data interference	ART.44 of Romania Law no 161/2003
Article 5 – System interference	ART.45 of Romania Law no 161/2003
Article 6 – Misuse of devices	ART.46 of Romania Law no 161/2003
Article 7 – Computer-related forgery	ART.48 of Romania Law no 161/2003
Article 8 – Computer-related fraud	ART.49 of Romania Law no 161/2003
Article 9 – Offences related to child pornography	ART.51(1) of Romania Law no 161/2003
Title 4 – Offences related to infringements of copyright and related rights	
Article 10 – Offences related to infringements of copyright and related rights	ART. 139^{8} - 139^{9} and art. 143 of Law on copyright no.8/1996
Article 11 – Attempt and aiding or abetting	For ART. 11 (1) of the Convention on Cybercrime – ART. 23, ART. 26, ART. 27 of Criminal Code For ART. 11(2) of Convention on Cybercrime – ART. 47, ART.50 and ART. 51(2) of Romania Law no 161/2003
Article 12 – Corporate liability	ART. 19^{1} of Criminal Code (amended by Law no 278/2006) Article 12 – partially covered
Article 13 – Sanctions and measures	For art. 13(1) of Convention on Cybercrime - ART. 42-46, ART.48-49 and ART. 51 of Romania Law no 161/2003 For art. 13(2) of Convention on Cybercrime – ART. 53^{1} of Criminal Code (amended by Law no 278/2006)
Section 2 – Procedural law	
Article 14 – Scope of procedural provisions	ART. 58 of Romania Law no 161/2003
Article 15 – Conditions and safeguards	ART. 26 (1), 27 (3), 28 of Romania Constitution, ART. 91^{1} Criminal procedure Code, ART. 57 (1), (2) of Romania Law no 161/2003, ART. 3 (3), (5) of Romania Law no 365/2002 on electronic commerce (amended by Law no 121/2006)
Article 16 – Expedited preservation of stored	ART.54 of Romania Law no 161/2003

computer data	
Article 17 – Expedited preservation and partial disclosure of traffic data	ART.54 of Romania Law no 161/2003
Article 18 – Production order	ART. 16 of Law no 508/2004 on establishing, organizing and operating of the Directorate for Investigation of the Organized Crime and Terrorism Offences
Article 19 – Search and seizure of stored computer data	For art. 19 (3) of Convention on Cybercrime – ART. 55 of Romanian Law 161/2003(in view of making copies that can serve as evidence); ART. 96 and Art.99 of Criminal procedure Code. For art.19 (1-2) of Convention on Cybercrime - ART.56 (1) (3) of Romania Law no 161/2003.
Article 20 – Real-time collection of traffic data	It is considered to be implemented by the new draft of the Criminal Procedure Code
Article 21 – Interception of content data	ART.57 of Romania Law no 161/2003 ART. 91^1 (Section V^1) of the Criminal Procedure Code on audio and video interception and recording of conversations or communications by telephone or by any other electronic means of communication
Section 3 – Jurisdiction	
Article 22 – Jurisdiction	ART. 3-4 and art.142-143 Criminal Code
Chapter III – International co-operation	
Article 24 – Extradition	Art.23-24 (1) of Convention on cybercrime - ART.60 of Romania Law no 161/2003 and Title II of Law no. 302/2004 on international judicial co-operation in criminal matters as amended and supplemented by Law No. 224/2006
Article 25 – General principles relating to mutual assistance	ART.61 of Romania Law no 161/2003
Article 26 – Spontaneous information	ART.66 of Romania Law no 161/2003 and ART. 166 of Law no. 302/2004 on international judicial co-operation in criminal matters as amended and supplemented by Law No. 224/2006
Article 27 – Procedures pertaining to mutual assistance requests in the absence of applicable international agreements	Single article (2) b) of Law no 64/2004 for ratification of the Council of Europe Convention on cybercrime
Article 28 – Confidentiality and limitation on use	ART. 12 of Law no. 302/2004 on international judicial co-operation in criminal matters as amended and supplemented by Law No. 224/2006
Article 29 – Expedited preservation of stored computer data	ART.63 of Romania Law no 161/2003
Article 30 – Expedited disclosure of preserved traffic data	ART.64 of Romania Law no 161/2003
Article 31 – Mutual assistance regarding accessing of stored	ART. 60 of Romania Law no 161/2003

computer data	
Article 32 – Trans-border access to stored computer data with consent or where publicly available	ART.65 of Romania Law no 161/2003
Article 33 – Mutual assistance in the real-time collection of traffic data	ART. 60 of Romania Law no 161/2003
Article 34 – Mutual assistance regarding the interception of content data	ART. 60 of Romania Law no 161/2003
Article 35 – 24/7 Network	ART. 62 of Romania Law no 161/2003
Article 42 – Reservations	*No need to fill in this information as it will be copied from the Council of Europe treaty data base*

Appendix 1: **solutions in national legislation**

Romania Law no 161/2003

Title III on preventing and fighting cybercrime[1]

Chapter I

General Provisions

Art. 34 – The present title regulates the prevention and fighting of cybercrime by specific measures to prevent, discover and sanction the infringements through the computer systems, providing the observance of the human rights and the protection of personal data.

Art. 35 - (1) For the purpose of the present law, the terms and phrases below have the following meaning:

a) *„computer system"* means any device or assembly of interconnected devices or that are in an operational relation, out of which one or more provide the automatic data processing by means of a computer program;

b) *„automatic data processing"* is the process by means of which the data in a computer system are processed by means of a computer program;

c) *„computer program"* means a group of instructions that can be performed by a computer system in order to obtain a determined result;

d) *„computer data"* are any representations of facts, information or concepts in a form that can be processed by a computer system. This category includes any computer program that can cause a computer system to perform a function;

e) *„a service provider"* is:

1. any natural or legal person offering the users the possibility to communicate by means of a computer system;

2. any other natural or legal person processing or storing computer data for the persons mentioned in paragraph 1 and for the users of the services offered by these;

f) *„traffic data"* are any computer data related to a communication by means of a computer system and generated by this, which represent a part in the chain of communication,

[1] The relevant provisions for preventing, discovering and sanctioning the offences committed through the computer systems are incorporated in Title III of the Law 161/2003 on certain measures to ensure transparency in the exercise of public dignity, public office and in the business environment, to prevent and sanction corruption (published in the Official Gazette no 279 from 21 April 2003)

indicating the communication's origin, destination, route, time, date, size, volume and duration, as well as the type of service used for communication

g) *"data on the users"* are represented by any information that can lead to identifying a user, including the type of communication and the serviced used, the post address, geographic address, IP address, telephone numbers or any other access numbers and the payment means for the respective service as well as any other data that can lead to identifying the user;

h) *„security measures"* refers to the use of certain procedures, devices or specialised computer programs by means of which the access to a computer system is restricted or forbidden for certain categories of users;

i) *„pornographic materials with minors"* refer to any material presenting a minor with an explicit sexual behaviour or an adult person presented as a minor with an explicit sexual behaviour or images which, although they do not present a real person, simulates, in a credible way, a minor with an explicit sexual behaviour.

(2) For the purpose of this title, *a person acts without right* in the following situations:

a) is not authorised, in terms of the law or a contract;
b) exceeds the limits of the authorisation;
c) has no permission from the competent natural or legal person to give it, according to the law, to use, administer or control a computer system or to carry out scientific research in a computer system.

Chapter II

Prevention of cybercrime

Art. 36 – In order to ensure the security of the computer systems and the protection of the personal data, the authorities and public institutions with competence in the domain, the service providers, the non-governmental organisations and other representatives of the civil society carry out common activities and programs for the prevention of cybercrime.

Art. 37 – The authorities and public institutions with competence in the domain, in collaboration with the service providers, the non-governmental organisations and other representatives of the civil society promote policies, practices, measures, procedures and minimum standards for the security of the computer systems.

Art. 38 - The authorities and public institutions with competence in the area, in collaboration with the service providers, the non-governmental organisations and other representatives of the civil society organise informing campaigns on cybercrime and the risks the users of the computer systems.

Art. 39 – (1) The Ministry of Justice, The Ministry of Interior, the Ministry of Communications and Information Technology, Romanian Intelligence Service and Foreign Intelligence Department establish and permanent up-date a database on cybercrime.
(2) The National Institute of Criminology under the subordination of the Ministry of Justice

carries out periodic studies in order to identify the causes determining and the conditions favouring the cybercrime.

Art. 40 - The Ministry of Justice, The Ministry of Interior, the Ministry of Communications and Information Technology, Romanian Intelligence Service and Foreign Intelligence Department carry out special training programs for the personnel with attributions in preventing and fighting cybercrime.

Art. 41 – The owners or administrators of computer systems for which access is forbidden or restricted to certain categories of users are obliged to warn the users on the legal access and use conditions, as well as on the legal consequences of access without right to these computer systems.

Chapter III

Crimes and contraventions

Section 1

Offences against the confidentiality and integrity of computer data and systems

Art. 42 – (1) The access without right to a computer system is a criminal offence and is punished with imprisonment from 6 months to 3 years or a fine.

(2) Where the act provided in paragraph (1) is committed with the intent of obtaining computer data the punishment is imprisonment from 6 months to 5 years.

(3) Where the act provided in paragraphs 1-2 is committed by infringing the security measures, the punishment is imprisonment from 3 to 12 years.

Art. 43 – (1) The interception without right of non-public transmissions of computer data to, from or within a computer system is a criminal offence and is punished with imprisonment from 2 to 7 years.

(2) The same punishment shall sanction the interception, without right, of electromagnetic emissions from a computer system carrying non-public computer data.

Art. 44 – (1) The alteration, deletion or deterioration of computer data or restriction to such data without right is a criminal offence and is punished with imprisonment from 2 to 7 years.

(2) The unauthorised data transfer from a computer system is punished with imprisonment from 3 to 12 years.

(3) The same punishment as in paragraph (2) shall sanction the unauthorised data transfer by means of a computer data storage medium.

Art. 45 – The act of causing serious hindering, without right, of the functioning of a computer system, by inputting, transmitting, altering, deleting or deteriorating computer data or by restricting the access to such data is a criminal offence and is punished with imprisonment from 3 to 15 years.

Art. 46 – (1) It is a criminal offence and shall be punished with imprisonment from 1 to 6 years.

a) the production, sale, import, distribution or making available, in any other form, without right, of a device or a computer program designed or adapted for the purpose of committing any of the offences established in accordance with Articles 42-45;
b) the production, sale, import, distribution or making available, in any other form, without right, of a password, access code or other such computer data allowing total or partial access to a computer system for the purpose of committing any of the offences established in accordance with Articles 42 - 45;

2) The same penalty shall sanction the possession, without right, of a device, computer program, password, access code or computer data referred to at paragraph (1) for the purpose of committing any of the offences established in accordance with Articles 42-45.

Art. 47 – The attempt to commit the offences provided in Articles 42-46 shall be punished.

Section 2

Computer-related offences

Art. 48 – The input, alteration or deletion, without right, of computer data or the restriction, without right, of the access to such data, resulting in inauthentic data, with the intent to be used for legal purposes, is a criminal offence and shall be punished with imprisonment from 2 to 7 years.

Art. 49 – The causing of a loss of property to another person by inputting, altering or deleting of computer data, by restricting the access to such data or by any interference with the functioning of a computer system with the intent of procuring an economic benefit for oneself or for another shall be punished with imprisonment from 3 to 12 years.

Art. 50 – The attempt to commit the offences provided in Articles 48 and 49 shall be punished.

Section 3

Child pornography through computer systems

Art.51 – (1) It is a criminal offence and shall be punished with imprisonment from 3 to 12 years and denial of certain rights the production for the purpose of distribution, offering or making available, distributing or transmitting, procuring for oneself or another of child pornography material through a computer system, or possession, without right, child pornography material in a computer system or computer data storage medium.

(2) The attempt shall be punished.

Section 4

Contraventions

Art. 52 – The non-observance of the obligation stipulated by art. 41 is a contravention and shall be sanctioned by a fee between 5.000.000 lei and 50.000.000 lei.

Art. 53 – (1) Finding a contravention provided in art. 52 and the application of the sanction are performed by the personnel authorised for this purpose by the minister of communications and IT as well as by the specially authorised personnel within the Ministry of Interior.

(2) The provisions of Government Ordinance no. 2/2001 on the legal regime of contraventions, approved with amendments by Law no.180/2002 are applicable.

Chapter IV

Procedural provisions

Art. 54 - (1) In urgent and dully justified cases, if there are data or substantiated indications regarding the preparation of or the performance of a criminal offence by means of computer systems, for the purpose of gathering evidence or identifying the doers, the expeditious preservation of the computer data or the data referring to data traffic, subject to the danger of destruction or alteration, can be ordered.

(2) During the criminal investigation, the preservation is ordered by the prosecutor through a motivated ordinance, at the request of the criminal investigation body or ex-officio, and during the trial, by the court order.

(3) The measure referred to at paragraph (1) is ordered over a period not longer than 90 days and can be exceeded, only once, by a period not longer than 30 days.

(4) The prosecutor's ordinance or the court order is sent, immediately, to any service provider or any other person possessing the data referred to at paragraph (1), the respective person being obliged to expeditiously preserve them under confidentiality conditions.

(5) In case the data referring to the traffic data is under the possession of several service providers, the service provider referred to at paragraph (4) has the obligation to immediately make available for the criminal investigation body or the court the information necessary to identify the other service providers in order to know all the elements in the communication chain used.

(6) Until the end of the criminal investigation, the prosecutor is obliged to advise, in writing, the persons that are under criminal investigation and the data of whom were preserved.

Art. 55 – (1) Within the term provided for at art. 54 paragraph (3), the prosecutor, on the basis of the motivated authorisation of the prosecutor specially assigned by the general prosecutor of the office related to the Court of Appeal or, as appropriate, by the general prosecutor of the office related to the Supreme Court, or the court orders on the seizing of the objects containing computer data, traffic data or data regarding the users, from the person or service provider possessing them, in view of making copies that can serve as evidence.

(2) If the objects containing computer data referring to the data for the legal bodies in order to make copies, the prosecutor mentioned in paragraph (1) or court orders the forced seizure. During the trial, the forced seizure order is communicated to the prosecutor, who takes measures to fulfil it, through the criminal investigation body.

(3) The copies mentioned in paragraph (1) are achieved by the technical means and the proper procedures to provide the integrity of the information contained by them.

Art.56 – (1) Whenever for the purpose of discovering or gathering evidence it is necessary to investigate a computer system or a computer data storage medium, the prosecutor or court can order a search.

(2) If the criminal investigation body or the court considers that seizing the objects that contain the data referred to at paragraph (1) would severely affect the activities performed by the persons possessing these objects, it can order performing copies that would serve as evidence and that are achieved according to art. 55, paragraph (3).

(3) When, on the occasion of investigating a computer system or a computer data storage medium it is found out that the computer data searched for are included on another computer system or another computer data storage medium and are accessible from the initial system or medium, it can be ordered immediately to authorize performing the search in order to investigate all the computer systems or computer data storage medium searched for.

(4) The provisions of the Criminal Procedure Code regarding searches at home are applied accordingly.

Art.57 – (1) The access to a computer system, as well as the interception or recording of communications carried out by means of computer systems are performed when useful to find the truth and the facts or identification of the doers cannot be achieved on the basis of other evidence.

(2) The measures referred to at paragraph (1) are performed by motivated authorisation of the prosecutor specially assigned by the general prosecutor related to the Court of Appeal or, as appropriate, of the general prosecutor of the office related to the Supreme Court, and for the corruption offences, of the general prosecutor of the National Anti-Corruption Office, by the criminal investigation bodies with the help of specialised persons, who are obliged to keep the confidentiality of the operation performed.

(3) The authorisation referred to at paragraph (2) is given for 30 days at the most, with the extension possibility under the same conditions, for duly justified reasons, each extension not exceeding 30 days. The maximum duration of these measures is 4 months.

(4) Until the end of the criminal investigation, the prosecutor is obliged to inform, in writing, the persons against whom the measures referred to in paragraph (1) are taken.

(5) The procedures of the Criminal procedure Code regarding the audio or video recordings are applied accordingly.

Art.58 – The provisions of this chapter are applicable to criminal investigations or during the trial for the offences stipulated in this title or any other offences committed by means of computer systems.

Art.59 – For the criminal offences stipulated in this title and any criminal offences committed by means of computer systems, in order to ensure the special seizure stipulated at art.118 of the Criminal Code it can be performed the prevention measures provided for by the Criminal Procedure Code.

Chapter V

International Cooperation

Art.60 – (1) The Romanian legal authorities cooperate directly, under the conditions of the law and by observing the obligations resulting from the international legal instruments Romania is Party of, with the institutions with similar attributions in other states, as well as with the international organisations specialised in the domain.

(2) The cooperation, organised and carried out according to paragraph (1) can have as scope, as appropriate, international legal assistance in criminal matters, extradition, the identification, blocking, seizing or confiscation of the products and instruments of the criminal offence, carrying out common investigations, exchange of information, technical assistance or of any other nature for the collection of information, specialised personnel training, as well as other such activities.

Art.61 – (1) At the request of the Romanian competent authorities or of those of other states, on the territory of Romania common investigations can be performed for the prevention and fighting the cybercrime.

(2) The common investigations referred to at paragraph (1) are carried out on the basis of bilateral or multilateral agreements concluded with the competent authorities.

(3) The representatives of the Romanian competent authorities can participate in common investigations performed on the territory of other states by observing their legislation.

Art.62 - (1) In order to ensure an immediate and permanent international cooperation in the cybercrime area, within the Organised Crime Fighting and Anti-drug Section of the Prosecutor's Office belonging to the Supreme Court, a service for combating cybercrime is established as a contact point permanently available.

(2) The Service for combating cybercrime has the following attributions:

a) provides specialised assistance and information on Romanian legislation in the area to similar contact points in other states;

b) orders the expeditious preservation of data as well as the seizure of the objects containing computer data or the data regarding the data traffic required by a competent foreign authority;

c) executes or facilitates the execution, according to the law, of letters rogatory in cases of combating cybercrime cooperating with all the competent Romanian authorities.

Art. 63 - (1) Within the international cooperation, the competent foreign authorities can require from the Service for combating cybercrime the expeditious preservation of the computer data or of the data regarding the traffic data existing within a computer system on the territory of Romania, related to which the foreign authority is to formulate a request of international legal assistance in criminal matters.

(2) The request for expeditious preservation referred to at paragraph (1) includes the following:
a) the authority requesting the preservation;

b) a brief presentation of facts that are subject to the criminal investigation and their legal background;

c) computer data required to be preserved;

d) any available information, necessary for the identification of the owner of the computer data and the location of the computer system;

e) the utility of the computer data and the necessity to preserve them;
f) the intention of the foreign authority to formulate a request of international legal assistance in criminal matters;

(3) The preservation request is executed according to art. 54 for a period of 60 days at the least and is valid until a decision is taken by the Romanian competent authorities, regarding the request of international legal assistance in criminal matters;

Art.64 - If, in executing the request formulated according to art.63 paragraph (1), a service provider in another state is found to be in possession of the data regarding the traffic data, the Service for combating cybercrime will immediately inform the requesting foreign authority about this, communicating also all the necessary information for the identification of the respective service provider.

Art.65 - (1) A competent foreign authority can have access to public Romanian sources of computer data without requesting the Romanian authorities.

(2) A competent foreign authority can have access and can receive, by means of a computer system located on its territory, computer data stored in Romania, if it has the approval of the authorised person, under the conditions of the law, to make them available by means of that computer system, without requesting the Romanian authorities.

Art. 66 – The competent Romanian authorities can send, ex-officio, to the competent foreign authorities, observing the legal provisions regarding the personal data protection, the information and data owned, necessary for the competent foreign authorities to discover the offences committed by means of a computer system or to solve the cases regarding these crimes.

Art.67 – Art.29 of Law no.365/2002 on e-commerce, published in the Official Journal of Romania, Part I, no.483 of May 7, 2002 is abrogated.

Constitution of Romania is available in English on http://www.cdep.ro

CRIMINAL CODE
Title II
OFFENCES

Chapter I
GENERAL PROVISIONS

Guilt

Art.19. (1) There is guilt when an act that represents a social danger is committed with intent or with negligence.
1. An act was committed with intent when the offender:
a) foresaw the outcome of his/her act, and intended for this outcome to take place by the commission of that act;
b) foresaw the outcome of his/her act and, although he/she did not intend it, accepts the possibility for it to take place.
2. An act was committed out of negligence when the offender:
a) foresaw the outcome of his/her act, but did not accept it, because he/she unfoundedly deemed it unlikely to take place;
b) did not foresee the outcome of his/her act, although he/she ought and would have been able to.
(2) An act that resides in an action committed with negligence shall be an offence only when the law provides this expressly.
(3) An act consisting of inaction shall be an offence regardless of whether it was committed with intent or with negligence, unless the law sanctions only its commission with intent.

Chapter III
PARTICIPATION

Participants

Art.23 - Persons who contribute to the commission of an act provided in the criminal law as authors, instigators or accomplices are participants.

Authors

Art. 24 - A person directly committing an act provided in the criminal law is an author.

Instigators

Art.25 - An instigator is a person who intentionally determines another person to commit an act provided in the criminal law.

Accomplices

Art.26 - (1) An accomplice is a person who intentionally facilitates or helps in any way in the commission of an act provided in the criminal law. A person who promises, either before or during the commission of the offence, to conceal the proceeds emerging from it or to favour the perpetrator, even if after commission of the offence the promise is not kept, shall also be an accomplice.

Penalty for participation

Art.27 - Instigators and accomplices to an act provided in the criminal law committed with intent shall be sanctioned by the penalty provided in the law for authors. In establishing the penalty, each person's contribution to the commission of the offence, as well as Art. 72, shall be taken into account.

THE CRIMINAL CODE amended by Law no 278/2006 (extract)

Conditions for the criminal liability of legal persons	ART. 19[1] Legal persons, with the exception of the State, the public authorities and the public institutions the activity of which is not the subject of private domain, shall be criminally liable for criminal offences committed in order to activate in their activity field or in the interest or on behalf of the legal person, provided that the act has been committed with the form of guilt provided in criminal law. Criminal liability of legal persons shall not exclude the criminal liability of natural persons who contributed in any manner to the perpetration of the same criminal offence."
Types of penalties applicable to legal persons	ART. 53[1] The penalties are: main and complementary. The main penalty is a fine from RON 2.500 to RON 2.000.000. Complementary penalties are: a) dissolution of the legal person; b) suspension of the activity of the legal person for a period from 3 months to one year or suspension of that of the activities of the legal person which served in the perpetration of the offence, for a period from 3 months to 3 years; c) closing of working locations belonging to the legal person, for a period from 3 months to 3 years; d) prohibition to participate in public procurement for a period from one to 3 years; e) display or broadcasting of the sentencing judgement.

CRIMINAL PROCEDURE CODE (extract)
Section V[1]
Audio or video interception and recording

ART. 91[1]

Conditions and cases of interception and recording of conversations or communications by telephone or by any other electronic means of communication

The interception and recording of conversations or communications by telephone or by any electronic means of communication are performed with the reasoned authorisation of a judge, at the request of the public prosecutor who is conducting or supervising criminal prosecution, under the law, in the event that solid data or clues indicate the preparation or perpetration of a criminal offence for which criminal prosecution is conducted ex officio, and interception and recording are required in order to establish the factual situation or because it would be impossible to identify or locate the participants by any other means or such means would cause much delay to the investigation.

Interception and recording of conversations or communications by telephone or by any electronic means of communication may be authorised for criminal offences against national security, as set forth in the Criminal Code and in other special laws, as well as for criminal offences of drug trafficking, weapons trafficking and trafficking in persons, terrorist acts, money laundering, counterfeiting of currency or other valuables, for the criminal offences set forth in Law No.78/2000 on the Prevention, Detection and Punishment of Acts of Corruption, as subsequently amended and supplemented, and for other serious criminal offences or criminal offences that are perpetrated through means of electronic communication. Para. 1 shall apply accordingly.

Authorisation shall be given for the period of time during which interception and recording is needed, however not for more than 30 days, in private by the president of the court that would be competent to try the case in first instance or of the court of the same rank that has jurisdiction over the prosecution office where the public prosecutor works who is conducting or supervising criminal prosecution. In the absence of the president of the court, the authorisation shall be given by a judge designated by the court president.

Such authorisation may be renewed, either before or after the previous one expires, but under the same conditions and for properly justified reasons. However, each extension may not exceed 30 days.

The total duration of authorised interception and recording, with regard to the same person and the same act may not exceed 120 days.

Recording of conversations between a lawyer and the party whom he is representing or assisting within the proceedings may not be used as evidence unless it contains or leads to the establishment of conclusive and useful data or information regarding the preparation or commission by the lawyer of a criminal offence of those provided in para. 1 and 2.

The public prosecutor ordains immediate cessation of interceptions and recordings before the expiry of the authorisation if the reasons that justified such measures no longer exist, and shall inform about this the law court that issued the authorisation.

At the reasoned request of the injured person, the public prosecutor may request authorisation from the judge to intercept and record conversations or communications by the injured person by telephone or by any electronic means of communication, whatever the nature of the criminal offence under investigation.

Interception and recording of conversations or communications shall be authorised by means of a reasoned order, which must include: the actual clues and facts that justify the measure; the reasons for which it would be impossible to determine the factual situation or to identify or locate the participants by other means or the reasons why the investigation would be very much delayed; the person, the means of communication or the place that is subject to recording; and the period for which interception and recording are authorised.

Law no. 508/2004 on establishing, organizing and operating of the Directorate for Investigation of the Organized Crime and Terrorism Offences *(amended by Emergency Ordinance of Government no. 131/2006).*

ART. 16

(2) The public prosecutors of the Directorate for Investigation of Offences of Organised Crime and Terrorism may ordain that they be communicated the originals or copies of any data, information, documents, banking, financial or accounting documents and other such items, by any person who holds them or from whom they emerge, and such person shall be bound to comply, under paragraph (1).

(3) Failure to observe the obligation in paragraph (2) shall entail judicial liability, under the law.

CRIMINAL PROCEDURE CODE (extract)

Confiscation of objects and writings	**Art. 96** - The criminal investigation body or the court must take away the objects or writings that may serve as means of evidence in the criminal trial.
Confiscation by force of objects or writings	**Art. 99** – If the object or writing required is not delivered voluntarily, the criminal investigation body or the court order confiscation by force. During the trial, the order of confiscation by force of objects or writings is communicated to the prosecutor, who takes enforcement measures through the criminal investigation body.

THE CRIMINAL CODE (extract)

Criminal Law personality

Art.4. Criminal law shall apply to offences perpetrated outside the Romanian territory, if the perpetrator is a Romanian citizen or if he/she, while having no citizenship, domiciles in this country.

Decisions of the Constitutional Court:

Territorial nature of Criminal Law Territory

Art.3. Criminal Law shall apply to offences committed on Romanian territory.

Art. 142. The term "territory" in the phrases "Romanian territory" and "the territory of our country" means the surface of land and water that is comprised by the borders, with the subsoil and the aerial space, as well as the territorial sea with its soil, subsoil and aerial space.

Offence committed on the territory of our country

Art. 143. (1) "Offence committed on the territory of our country" means any offence committed on the territory shown in Art. 142 or on Romanian ships or aircraft.

(2) An offence shall be deemed as committed on the territory of our country also when only an act of realisation was performed or only the result of the offence occurred on this territory or on Romanian ships or aircraft.

Law no 64/2004 for ratification of the Council of Europe Convention on cybercrime

In accordance with Article 27, paragraph 2.c, of the Convention, Romania declares that the central authorities responsible for sending and answering requests for mutual assistance are:

a) the Prosecutor's Office to the High Court of Cassation and Justice for the requests of judicial assistance formulated in pre-trial investigation (address: Blvd. Libertatii nr. 12-14, sector 5, Bucharest);

b) the Ministry of Justice for the requests of judicial assistance formulated during the trial or execution of punishment.

The Romanian Copyright Law No.8/1996 (extract)

ART. 139^8

There is a criminal offence and shall be punished with imprisonment from 1 to 4 years or a fine the act of making available to the public, including through the Internet or other computer networks, without the consent of the owners of the copyright of protected works, neighbouring rights or sui generis rights of the manufacturers of databases or copies of such protected work, regardless of the form of storage thereof, in such a manner as to allow to the public to access it from anywhere or at anytime individually chosen.

ART. 139^9

There is a criminal offence and shall be punished with imprisonment from 1 to 4 years or a fine the unauthorised reproduction in information systems of computer software in any of the following ways: install, storage, running or execution, display or intranet transmission.

ART. 143

(1) There is a criminal offence and shall be punished with imprisonment from 3 months to 3 years or a fine the act of manufacturing, import, distribution or rental, offer, by any means, for sale or rental or possession in view of selling without right devices or components that allow neutralisation of technical measures of protection or that perform services that lead to neutralisation of technical measures of protection or that neutralise such technical measures of protection, including in the digital environment.

(2) There is a criminal offence and shall be punished with imprisonment from 3 months to 3 years or a fine the act of person whom, without having the consent of the owners of the copyright, and while knowing or should have known that thus is allowing, facilitating, causing or concealing a violation of a right as set forth in this law:

a) removes or modifies from the protected works for commercial purposes any electronic information relating to the applicable regulations on copyright or neighbouring rights,

b) distributes, imports in view of distribution, broadcasts or publicly communicates or makes available to the public, so as to allow access from any place and at any time chosen individually, without right, through digital technology, works or other protected works for which the information existing in electronic form regarding the regulations on copyright or related rights, have been removed or modified without authorisation.

Table 1. Regulatory Framework

Regulator	Substantive Rules	Sanctions	Mechanism
1. The actor him/herself	Personal ethics	Self-sanction	Self
2. Second party controllers (i.e., the person acted upon)	Contractual provisions	Various self-help mechanisms	PICS, RSACi, filter software
3. Nonhierarchically organized social forces	Social norms	Social sanctions	Code of Conduct
4. Hierarchically organized nongovernmental organizations	Organization rules	Organization sanctions	Industry self-regulation
5. Governments	Law	State enforcement, coercive sanctions	Law

Adapted from Ellickson (1991) [31] and rpt. in Hwa Ang Peng, "How Countries Are Regulating the Internet Content," 20 Jan. 2009 <http://www.isoc.org/inet97/proceedings/B1/B1_3.HTM#s11>