American University of Armenia

Masters' thesis:

Cybercrime: The legislative regulation in Armenia: The shortcomings that lead to the non-compliance of State positive obligation towards individuals with respect of Personal Life and Freedom of Expression

LL.M program 2nd year student

Lilit Avagyan

Instructor: Siranush Sahakyan

Table of Contents

Introduction

The first personal computers became popular in 1980s of pervious century which led to the further development of computer systems. This new global digital environment created new pace of our activities in the local, regional and global field boosting political activism, broad cultural exchanges. At one point these activities are "not real", as they are virtual, but on the other side they are an essential and inseparable part of "real citizens" lives. As of today we actively share different types of information on the Internet; put "comments" in social websites, "likes" in Facebook, My Space, simultaneously freely expressing our thoughts and exercising our human rights. It is an unequivocal fact that today internet is a vital part of our lives. As The UN Special Rapporteur on Freedom of Expression rightly stresses that: "access to the Internet and other digital means of communication has become essential to full and free participation in social, cultural and political life".[1] In the 21st century internet access does not necessarily means fixed personal computers, but also mobile devices – laptops, tablets. E-mails have displaced traditional letters[2]. Our real, offline lives and virtual, online lives are ever more intertwined. In just over a decade, this technological miracle has brought societies the world over closer together than in the whole history of international relations. Information legally made available in one country was available globally – even in countries where the publication of such information was criminalized.[3] But with all new wonders, also come new worries. The global character of internet shifted the originally local crimes into transnational crimes. Besides all the miracles, this new global digital environment became a new arena for unlawful behavior: dissemination of hate

[1] Second report of the UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue, dated 10 August 2011, UN Document A/66/290, paras. 10ff. and 78, available at: www.ohchr.org/Documents/Issues/Opinion/A.66.290.pdf, [last access: 1 May 2016 at 5:04 pm].
[2] www.defenselink.mil/transcripts/transcript.aspx?transcriptid=3996, [last access: 25 April 2016 at 3:11 pm]
[3] Sofaer/Goodman- The Transnational Dimension of Cyber Crime and Terrorism, 2001, page 7

speech, child pornography, incitement to violence, identity theft, fraud, money laundering, terrorism and new emerging cybercrimes. The criminal abuse of information technology and appropriate legal response is an important issue which have discussed in an international and national level over the last 30 years.

We all know, that "Entering into the cyberspace requires going through certain private gatekeepers who control the content and the access to the public space of information and discussion".[4]

We can notice that growing interest towards latest computer technologies in Armenia accrues every day. Up-to-date social and public relations are very hard to imagine without internet web, social websites or e-mails. Having in mind this "internet" reality it is worth to examine cyber threats in Armenia. As the attacks techniques becoming more sophisticated to develop tools which respond adequately are indeed extremely difficult. The target of this type of crimes varies from Government to Businesses, even individuals. Indeed, the attacks against information infrastructure and Internet services between individuals within a state are serious issues. It is always a challenge for the states to speedily expose the new, sophisticated ways of crimes, grasp their nature and to respond them. In this new reality the existing legal concepts challenged, as the flow of information and communications take place easily, borders are no longer boundaries to this flow and crimes produce their effects other than their location. However, domestic laws are generally confined to a specific territory. Thus, solutions to the problems posed must be addressed by international law, through adequately adopted international legal instruments and consequent ratification and follow-up by the states. As one chain of this changing environment, Armenia must also define clear and concise techniques as well as proper legislation for fighting against cybercrime, simultaneously, vigorously acting and cooperating with international level thereby reducing all the imminent threats to the minimum. Even though it is difficult to control or prevent cybercrimes as the attackers are often times faceless, as the attacker can be in Austria or Nigeria can attempt fraud against Armenia is really matter and the complexity of the cybercrimes includes also the fact that IT sector develops more speedily than the protective mechanisms, nevertheless it is worth to explore Armenian legislative regulation of cybercrime, try to identify inadequacies and shortcomings; and try to bring new solutions and recommendations for further effective combat. Moreover, within the scope of this paper it is worth to explore the international instruments currently due in place, the level of compliance and to discuss the issue of relevant consequences of noncompliance to the international standards and inadequate internal regulation of cybercrime within the ambit of State positive obligation

[4] Yves Poullet, "Internet of the future: achieving transparency, pluralism and democracy", November 2009, available at www.crids.eu/recherche/publications/textes/internet-of-the-future/at_download/file

provided by ECHR Article 8 (Right to respect for private and family life) and Article 10 (Freedom of expression).

Chapter 1

The nature and various tools to commit Cybercrime: The Budapest Convention on Cybercrime

Currently, the universal definition of the term "Cybercrime" does not exist. Connected with the existing diverse environments and scenarios various attempts tried to give a definition in a more or less broad or narrow sense.

United Nations' Definition of Cybercrime:

"Cybercrime spans not only state but national boundaries as well. At the Tenth United Nations Congress on the Prevention of Crime and Treatment of Offenders, in a workshop devoted to the issues of crimes related to computer networks, cybercrime was broken into two categories and defined thus:

- Cybercrime in a narrow sense (computer crime): Any illegal behavior directed by means of electronic operations that targets the security of computer systems and the data processed by them.
- Cybercrime in a broader sense (computer-related crime): Any illegal behavior committed by means of, or in relation to, a computer system or network, including such crimes as illegal possession [and] offering or distributing information by means of a computer system or network."[5]

One common definition describes cybercrime as any activity in which computers or networks are a tool, a target or a place of criminal activity.[6] Another broader definition is provided by The

[5] Scene of the Cybercrime, Second Edition, Littlejohn Shinder and Michael Cross, July 21, 2008 / 10th UN Congress on the Prevention of Crime and the Treatment of Offenders, 2000, A/CONF.187/10, page 5; available at: www.uncjin.org/Documents/congr10/10e.pdf.

[6] Goodman, Why the Policy don't care about Computer Crime, Harvard Journal of Law & Technology, Vol. 10, No. 3; page 469.

Stanford Draft International Convention to Enhance Protection from Cyber Crime and Terrorism (the "Stanford Draft"),[7] which points out that cybercrime refers to acts in respect to cyber systems. Some definitions try to take objectives or intentions into account and define cybercrime more precisely[8], such as "computer-mediated activities which are either illegal or considered illicit by certain parties and which can be conducted through global electronic networks".[9]

And the U.S. Department of Justice expands the definition by stating: "any illegal activity that uses a computer for the storage of evidence".[10]

Cybercrime also defined as crime committed on the internet using the computer as either a tool or a targeted victim. But this separation into two distinct groups is very ambiguous, as many crimes evolve on a daily basis. Anyway, in order the offence to qualify as cybercrime it must enclose within a computer and a person behind it. The difference is about who is the main target. Hence, the computer will be looked at as either a target or tool for simplicity's sake.

- **Computer as a tool**

in this scenario the target is the individual and computer only a tool for Cybercrime, which triggers the victims' psychology-emotional weaknesses, rather than technical expertise.

- **Computer as a target**

unlike the previous one, these crimes implemented due to the technical knowledge of the offenders, as here computer is a tool and facilitator for the crime. These crimes emergence connected with the boom of informational technologies, but committed on a daily basis in a contemporary world. [11]

Development of software tools:

Access to a computer system is often not the primary motivation of an attack.[12] After a successful attack, offenders can include the computer in their botnet and use the computer for further criminal activities.[13]

By saying botnets we understand:

" A network of computers that have been infected by malicious software (computer virus). Such a network compromised computers ('zombies') may be activated to perform specific actions, such as attacking information system (cyber-attacks). Theses 'Zombies' can be controlled

[7] Goodman/Brenner, The Emerging Consensus on Criminal Conduct in Cyberspace, UCLA Journal of Law and Technology, Vol. 6, Issue 1, 2002, page 70, available at: www.lawtechjournal.com/articles/2002/03_020625_goodmanbrenner.pdf;

[8] Hayden, Cybercrime's impact on Information security, Cybercrime and Security, IA-3, page 3, 14 May 2006

[9] Hale, Cybercrime: Facts & Figures Concerning this Global Dilemma, CJI 2002, Vol. 18, available at: www.cjcenter.org/cjcenter/publications/cji/archives/cji.php?id=37, 17 August 2010

[10] http://searchsecurity.techtarget.com/definition/cybercrime

[11] Aghatise E. Joseph, Source: Computer Crime Research Center , June 28, 2006, available at http://www.crime-research.org/articles/joseph06/

[12] Walden, Computer Crimes and Digital Investigations, 2006, Chapter 3. 250.

[13] Wilson, Botnets, Cybercrime, and Cyberterrorism: Vulnerabilities and Policy Issues for Congress, 2007, page 4, available at: www.fas.org/sgp/crs/terror/RL32114.pdf.

often without a knowledge of the users of the compromised computers by another computer. This controlling computer is also known "command and control centre". [14]

One of the most proliferated type of cybercrime is Troyan horse virus (which comes from a Greek fable) when the potential victim unknowingly downloads the virus sent by an email where it masquerades as an image or joke, or by a malicious website, which installs a keystroke logger to the victim's computer. The keystroke logger embedded to the personal computer is starting to steal private data (internet banking and email passwords).[15] Unlike viruses and worms, Trojan horses cannot spread by themselves. The Trojan horse lurks silently on the infected machine, invisibly carrying out its misdeeds even when the victim continues on with their normal activities.[16]

But before going forward let us understand the essence of "personal data".

Article 2 (a) of EU Data Protection Directive 95/46/EC prescribes personal data in the following way:

"'personal data' shall mean any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity;"[17]

According to Article 2 Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data;

Under the Directive on Privacy and Electronic Communications;

"Personal data means data relating to a living individual who is or can be identified either from the data or from the data in conjunction with other information that is in, or is likely to come into, the possession of the data controller."[18]

Thus, having regard all the definitions cited above we can conclude that data is personal, when someone is capable to address the information to a person which can comprise address, bank statements, criminal record, credit card number, social security number, etc.

---

[14] Directive on attacks against information systems, Strasbourg, 4 July 2013, http://europa.eu/rapid/press-release_MEMO-13-661_en.htm ,[last access: 2 May 2016 at 4:04 pm].

[15] Netadmintools Keylogging, available at: www.netadmintools.com/part215.htm

[16] http://us.norton.com/cybercrime-Trojansspyware ,[last access: 24 April 2016 at 2:56 pm].

[17]Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data; http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.1995.281.01.0031.01.ENG [last access: 30 April 2016 at 5:12 pm].

[18] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002, available at: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0058:en:HTML [last access: 24 April 2016 at 3:44pm]

In recent times the key crime in cyberspace is "phishing."[19] "The term means to "phish" for passwords and financial data from a sea of Internet. In this type of cybercrime the victim receives a supposedly legitimate email ("spoofing sites"), usually shaped in a way to seem authentic, as the URL has been masked so the Web address looks real and pretended to come from a well-known and trusted company.

The Spyware is a mean to covertly monitor activities on PCs for the purpose of gathering personal information, such as usernames, passwords, account numbers, files, and social security numbers. When the information already gathered it transmits it into another computer, usually for advertising purposes.[20] When you install a "free" music or file sharing service or download a screensaver, it is probably you also installed with it a spyware.[21]

As any cybercrime relates to theft or manipulation of data, "Spam" is another technique. It is conducted by the emission of unsolicited bulk messages. The E-mails contains advertisements for products and services. Spam e-mails are highly profitable as the cost of sending out billions of e-mails is low – and even lower where botnets are involved.[22]

Computer worms are self-replicating computer programs that harm the network by initiating multiple data-transfer processes.[23] They influence the whole network but do not target any specific computer systems. Unlike worms, DoS ("denial of service" attack) and DDOS ("distributed denial of service") target specific computer systems. The malicious modifies or destroys data, which is a really serious threat[24]. Under this attack a computer system becomes unavailable for users. This may include saturating the target computers or networks with external communication requests, thereby hindering service to legitimate users.

Conceptually, ID theft can be separated into three distinct phases:

- Phase 1 The obtaining of identity information through physical theft, through search engines, insider attacks, attacks from outside (illegal access to computer systems, Trojans, keyloggers, spyware and other malware) or through the use of phishing and or other social engineering techniques.
- Phase 2 The possession and disposal of identity information, which includes the sale of such information to third parties.

---

[19] Jakobsson, The Human Factor in Phishing, 2007, available at: www.informatics.indiana.edu/markus/papers/aci.pdf

[20] The Crimeware Landscape: Malware, Phishing, Identity Theft and Beyond, available at: www.antiphishing.org/reports/APWG_CrimewareReport.pdf.

[21] http://us.norton.com/cybercrime-trojansspyware , [last access: 5 April 2016 at 05:19 pm]

[22] ITU Survey on Anti-Spam Legislation Worldwide 200 , available at: www.itu.int/osg/spu/spam/legislation/Background_Paper_ITU_Bueti_Survey.pdf,[last access: 1 May 2016 at 8:02]

[23] Shoch/Hupp- : http://vx.netlux.org/lib/ajm01.htm,

[24] Bryan Harris/Eli Konikoff /Phillip Petersen, Breaking the DDoS Attack Chain, CMU-ISR-MITS-2, August 2013, available at https://www.cmu.edu/mits/files/breaking-the-ddos-attack-chain.pdf

- Phase 3 The use of the identity information to commit fraud or other crimes, for example by assuming another's identity to exploit bank accounts and credit cards, create new accounts, take out loans and credit, order goods and services or disseminate malware. [25]

Furthermore, cybercrime tends to be much more serious and covers things such as cyberstalking and harassment, child predation, extortion, blackmail, stock market manipulation, complex corporate espionage, and planning or carrying out terrorist activities.[26]

The progressive pace of technologies is so fast that makes challenges for the legislative bodies and governmental authorities to respond timely and comprehensively. However, within this run several international conventions have already tried to deal with these new and complex issues in order to adopt an appropriate framework.

Budapest Convention on Cybercrime:

As already mentioned above the new informational society has created such an environment that existing legal concepts are challenged, particularly, criminals are located in a place which critically differs from the effects of their illegal acts. Therefore, to reach to the solutions that are effective to the problems pose must be priority of international law and new adequate international legal instruments must be adopted. For the global response of the threats of cybercrime the implementation of holistic cybercrime legislation was essential and fundamental step for the effective unified combat. The purpose of Budapest Convention on Cybercrime is to meet this challenge, with due respect to human rights in the new Information Society.

The main objective of Convention as preamble reads is to pursue a common criminal policy aimed at the protection of society against cybercrime, particularly by adopting appropriate legislation and fostering international co-operation.[27]

The Cybercrime Convention "uses technology- neutral language, in order to insure application of substantive criminal law offences to the current and future developments, aiming that new forms of malware or crimes also be covered by the Convention."[28]

Convention sets out it aims which includes first of all (1) harmonization the domestic criminal substantive law elements of offences and connected provisions in the area of cybercrime (2) providing for domestic criminal procedural law powers necessary for the investigation and

[25] T-CY GUIDANCES NOTES, Adopted by the 8th, 9th and 12th Plenary of the T-CY, Strasbourg, France 8 December 2014, available at: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680468b06 [last access: 1 May 2016 at 9:04 pm]

[26] Zeviar-Geese, G. 1997-98. Gonzaga Journal of International Law. Volume 1. 1997-1998

[27] Convention on Cybercrime, CETS No. 185, Budapest, 23.XI.2001; available at: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680081561, [last access: 6 April 2016 at 13:12pm]

[28] T-CY Guidance Note #2, Provisions of Budapest Convention covering botnets, Adopted by the T-CY at its 9th Plenary, June 5, Strasburg, 2013, available at: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802e7094 [last access: 1April 2016 at 3:51]

prosecution of such offences as well as other offences committed by means of a computer system or evidence in relation to which is in electronic form (3) setting up a fast and effective regime of international co-operation. [29]

Substantive criminal law issues are posted in Section 1 of Chapter II which divided in 4 different categories. Title 1 devoted to – Offences against the confidentiality, integrity and availability of computer data and systems, which defines the following offences: Illegal access; illegal interception; data interference; system interference; misuse of devices; Title 2 – Computer-related offences reads as follows: computer-related forgery; computer related fraud; as two specific kinds of manipulation of computer systems or computer data. This proves the reality that in many countries certain traditional legal interests are not protected sufficiently against new forms of interference and attacks. Title 3 is about Content-related offences which encompass offences related to child pornography. Title 4 which refers to the offences related to copyright and related rights and the framework of title 5 is ancillary liability and sanctions[30]

The key requirement of offences is that it must be done "without right". It means, that conduct described is not always punishable per se, and can be justified where classical legal defenses are applicable (self-defense, consent necessity), as well as other excuses, justifications that lead to the exclusion of criminal liability under domestic law.

Furthermore, in order the criminal liability to apply the offence must be committed "intentionally."[31]

Furthermore, Section 2 of Chapter II sets out the procedural law issues. In particular, it refers to the offences conducted through computer system or electronic form of evidence. The safeguards, common conditions applicable to all procedural powers were established. Expedited preservation of stored data; expedited preservation and partial disclosure of traffic data; production order; search and seizure of computer data; real-time collection of traffic data; interception of content data consequently set out in the procedural part of the Convention: Chapter II ends with the jurisdiction provisions. [32]

Chapter III provisions devoted to mutual assistance and extradition rules. Concerning the traditional mutual assistance two situations exist: with legal basis, which generally to be carried out to the terms of treaties, reciprocal legislation and arrangements, etc. in case of which the existing arrangements also apply to assistance under this Convention and without it where its

---

[29] Convention on Cybercrime, CETS No. 185, Budapest, 23.XI.2001; https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016800cce5b

[30] ETS 185 – Cybercrime (Convention), 23.XI.2001; https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680081561, [last access: 2April 2016 at 03:51pm]

[31] Ibid 1

[32] Ibid 2

provisions apply. Particularly, Article 23 sets forth for parties a provision to provide cooperation to each other "to the widest extent possible" and aims to minimize hindrances to the smooth and rapid flow of information and evidence internationally.

The Convention among other provisions provides that each Party has the obligation to designate a point of contact available 24 hours per day, 7 days per week as supplemental channels of existing police co-operation and mutual assistance modalities in order to ensure immediate assistance in investigations and proceedings. 24/7 point of contact, inter alia, facilitate or directly carry out the implementation of technical advice, collection of evidence, giving of legal information, preservation of data and locating of suspects[33]. This, undoubtedly, is an important step to the effective response to the challenges of computer and computer-related crimes.

In addition to establishing an international legal framework for cooperation, the Convention requires member states to implement just such holistic, compatible and convergent legislation. This is effected through principles enumerated in the various Articles of the Convention. Being a treaty instrument the Convention does not provide specific legislative language for implementation of the principles outlined by its provisions, although the language of the Convention has been used by a number of countries to draft domestic legislation. It thus, leaves the precise language for implementation of the principles enshrined in treaty obligations to the discretion of each sovereign member state. Thereby respecting the sovereignty of each member state as well as recognizing that each state varies in terms of its legal system and legislative process.

Chapter 2

International approaches to Cybercrime

Back to 1997, the Group of Eight (G8) was discussing the fight against cybercrime.[34] One of achievements was the development of an international 24/7-network of contacts requiring participating countries to establish points of contact for transnational investigations that are accessible 24 hours a day, 7 days a week which make regular summits[35].

[33] Ibid3

[34] ITU Global Cybersecurity Agenda / High-Level Experts Group, Global Strategic Report, 2008, page 17, available at: www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/index.html, [last access: 1 April 2016 at 11:51pm].

[35] UNCTAD/SDTE/ECB/2005/1, 2005, Chapter 6, page 233, available at: www.unctad.org/en/docs/sdteecb20051ch6_en.pdf,[last access: 5 April 2016 at 02:15pm].

The United Nations efforts have unique importance throughout its various resolutions addressed to cybercrime. The UN General Assembly adopted a resolution 45/121 dealing with computer-crime legislation.[36] Furthermore, the manual was issued in 1994.

The United Nations Resolutions 55/63 and 56/121 tried to address the problem of safe havens for those who criminally misuse information technologies by requesting that States put into place laws to eliminate such havens.[37] The two main UN General Assembly resolutions dealing with cybersecurity are Resolutions 57/239 and 58/199. They both emphasize the need for international cooperation in fighting cybercrime by recognizing that gaps in states' access to and use of information technologies can diminish the effectiveness of international cooperation in combating the criminal misuse of information technology.[38] The Resolution 60/177 stresses the need of harmonization in the fight against cybercrime[39]

The Resolution 64/211 passed in March 2010 was about the protection of critical information infrastructures, also resolution calls countries to review and update legal authorities (including those related to cybercrime, privacy, data protection, commercial law, digital signatures and encryption). Further it is called to the states to avail them for the review the regional, as well as international conventions

The International Telecommunication Union (ITU) is a specialized agency within the United Nations, which plays a leading role in the standardization and development of telecommunications as well as cybersecurity issues.[40]

In 1981, a Convention for the protection of individuals with regard to the automatic processing of personal data (Convention 108)[41] came into place. Data-protection laws regulate the use of personal data, Data protection as a new fundamental right, *sui generis*, linked to the protection of privacy. The aim is to protect the person's rights and interests against the processing of their information obtained from using computers.[42] Than Directive 95/46/EC was adopted in 1995,

---

[36] A/RES/45/121, adopted by the UN General Assembly on 14 December 1990, available at: www.un.org/documents/ga/res/45/a45r121.htm, [last access: 4 March 2016 at 12:24pm].

[37] A/RES/55/63, adopted by the UN General Assembly on12 December 2000, available at: www.unodc.org/pdf/crime/a_res_55/res5563e.pdf [last access: 5 April 2016 at 05:19 pm]

[38] A/RES/57/239, on Creation of a global culture of cybersecurity;
A/RES/58/199, on Creation of a global culture of cybersecurity and the protection of critical information infrastructure, available at: https://www.itu.int/ITU-D/cyb/cybersecurity/docs/UN_resolution_58_199.pdf [last access: 3 April 2016 at 07:07 pm]

[39] Declaration Synergies and Responses: Strategic Alliances in Crime Prevention and Criminal Justice, 2005, available at: www.unodc.org/pdf/crime/congress11/BangkokDeclaration.pdf.

[40] http://www.itu.int/en/Pages/default.aspx

[41] CoE, Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Council of Europe, CETS No. 108, 28 January 1981, available at: http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108 , [last access: 2 May at 03:14 pm]

[42] Ibid

which aims to protect processing of personal data and on the free movement[43]. The EU is set to adopt new data protection legislation in early 2016 which allows the transfer of data to states that are considered to have adequate data privacy safeguards. EU citizens can personal data to the third countries with strong protection. The list is limited to countries reported in 2016.[44]

The Council of Europe Recommendation No. R (89) 9 on Computer-Related Crime, which recognizes the need to respond rapidly and effectively to new technologies crimes. Also, the Committee of Ministers adopted Recommendation No. R (95) 13 concerning criminal procedure law for information technology crimes.

The abovementioned Convention on Cybercrime was opened for signature at 2001 by Council of Europe, which includes non-CoE states also. It is the most important regional instrument for fight against cybercrime. The Additional Protocol to the Convention on Cybercrime is concerning the criminalization of acts of a racist and xenophobic nature committed through computer systems[45].

Besides, many Model Laws on Cybercrime implemented which aimed to bridge the best practices already enunciated by the Convention. In 2002 a ***"Commonwealth Model Law"*** was based upon the Budapest Convention[46] and received much recognition as a first effort at a model law based upon the Convention received much recognition. The leaders acknowledge that coordination within and across the regions is essential in case policies, legislation and practices are so various as to constitute an impediment to the development of competitive regional markets.[47]

ITU in its global ITUEC-ACP project[48] focused to the three regions: Africa, the Caribbean and the Pacific islands (ACP).[49] First of all, ***HIPCAR*** Project objective is assess existing legislation of beneficiary States and compare them with international best practice and to draw up guidelines and model legislative texts in order to enhance competitiveness and socio-economic development in the Caribbean Region through the harmonization of information and communication technology (ICT) policies, legislation and regulatory procedures. Thus, to make

---

[43] Directive 95/46/EC, 23 November 1995, available at: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.1995.281.01.0031.01.ENG, [last access: 15 April at 12:04 am]

[44] https://secure.edps.europa.eu/EDPSWEB/edps/EDPS/Dataprotection/QA/QA2

[45] ETS No. 189, available at: http://conventions.coe.int, [last access: 16 April at 12:24 am]

[46] LMM(02)17 – Report to Law Ministers @ page 1, available at: http://www.cybercrimelaw.net/documents/%7BDA109CD2-5204-4FAB-AA77-86970A639B05%7D_Computer%20Crime.pdf

[47] Cybercrime Model Laws, Discussion paper prepared for the Cybercrime Convention Committee (T-CY), Strasbourg, France, 23 December 2014, available at: https://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/TCY/2014/3021_model_law_study_v15.pdf. [last seen 3 April 08:12 pm]

[48] HIPCAR Cybercrime/e-Crimes: Model Policy Guidelines & Legislative Texts Acknowledgements @ page iii

[49] http://www.itu.int/en/ITU-D/Projects/ITU-EC-ACP/Pages/default.aspx

an environment which will enable "ICT development and connectivity and ultimately will facilitate the integration of market, will promote to investment in modified and improved ICT services and capabilities, and will intensify the protection of ICT consumers' interests across the region".[50]With regard to cybercrime, the issue of harmonizing national legislations is highly relevant as a majority of countries base their mutual legal assistance regime on the principle of "dual criminality".[51] Therefore, the harmonization process is a key requirement for the aim to fill existing gaps in the national legislations and also enhance the cooperation among the beneficiary States.

The implementation of ITU-EC project on Capacity Building and ICT policies, Regulations and Legislative Framework for Pacific Islands Countries was one among this row of models.[52]

The AU Convection on Cyber Security and Persona Data Protection was adopted in 2014.[53] The Draft Reports prepared in 2008,[54] inter alia, raised the concerns about emerging questions that needed to be responded properly; "tracing and combating of cybercrime in all its forms (hacking, virus propagation, denial of service attacks, credit card fraud, etc)". The main objective of the current Convention is the harmonization of the laws of African States on electronic commerce, data protection, cyber security promotion and cybercrime control. The Convention recognizes that cybercrime "constitutes a real threat to the security of computer networks and the development of the Information Society in Africa".[55] To a great extent, the Convention adopts a holistic approach to cyber security governance by imposing obligations on Member States to establish national legal, policy and institutional governance mechanisms on cyber security.[56]

---

[50] http://www.itu.int/en/ITU-D/Projects/ITU-EC-ACP/HIPCAR/Documents/FINAL%20DOCUMENTS/ENGLISH%20DOCS/e-transactions_mpg.pdf

[51] Dual criminality exists if the offence is a crime under both the requestor and requesting party's laws. With regard to the dual criminality principle in international investigations, see: "United Nations Manual on the Prevention and Control of Computer-Related Crime", 269; Schjolberg/Hubbard, "Harmonizing National Legal Approaches on Cybercrime", 2005, page 5.

[52] Cybercrime Model Laws, Discussion paper prepared for the Cybercrime Convention Committee (T-CY), Strasbourg, France, 23 December 2014, available at: https://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/TCY/2014/3021_model_law_study_v15.pdf, [last access: 7 April 2016 at 05:19 pm]

[53] African Union (AU) Convention on Cyber Security and Personal Data Protection, EX.CL/846(XXV) 27th June 2014, available at: http://textlab.io/doc/1049289/convention-on-cyber-security-and-personal-data-protection [last access: 7 April 05:43 pm]

[54] Draft Report , African Union: Addis Ababa, Ethiopia, March 2008, available at: http://www.au.int/en/sites/default/files/decisions/9562-assembly_en_31_january_2_february_2008_auc_tenth_ordinary_session_decisions_and_declarations.pdf

[55] Preamble, AU Convention on Cyber Security, available at: https://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/TCY/2014/3021_model_law_study_v15.pdf, [last access: 4 April at 12:53 am]

[56] Uchenna Jerome Orji, "Examining Missing Cybersecurity Governance Mechanisms in the African Union Convention on Cybersecurity and Personal Data Protection", Computer Law Review International, October, 2014, Issue 5, pp.131-132.

Cooperation under African Sub-Regional Legal Instruments on Cyber Security- ECOWAS Directive on Fighting Cybercrime was adopted in 2011.[57]The Directive imposes obligations on Member States to criminalize cybercrime[58] and also establishes a framework to facilitate international cooperation on cyber security. In this respect, article 33(1) of the Directive provides that:

"Where Member States are informed by another Member State of the alleged commission of an offence as defined under the Directive, such Member States "shall cooperate in the search for and establishment of that offence, as well as in the collection of evidence pertaining to the offence".[59]

The COMESA Model Cybercrime Bill- COMESA established a Model Cybercrime Bill in 2011[60] to provide a uniform framework as guidance for the development of cybercrime laws among Member States. Bill itself does not create for Member States binding obligations for criminalization of cybercrimes. It also establishes an elaborate guide for the development of general framework to facilitate international cooperation[61], extradition[62], and mutual assistance[63] and provides for the establishment of national 24/7 points of contact.[64]

Another Model law was- ***The SADC Model Law on Computer Crime and Cybercrime*** established in 2012[65] aiming to serve as development guidance of cyber security laws for Southern African Development Community (SADC) Member States, even though the fact that it does not impose any obligations on Members to establish cybercrime laws. However, Members that have established cyber security laws may rely on the SADC Protocol on Mutual Legal Assistance in Criminal Matters[66] and the Protocol on Extradition[67] to obtain international cooperation from other Members. Under the SADC Protocol on Mutual Assistance, Member

---

[57] ECOWAS Directive C/DIR.1/08/11 on Fighting Cybercrime, adopted at ECOWAS Council of Ministers at Abuja, Nigeria, August 2011, available at https://ccdcoe.org/sites/default/files/documents/ECOWAS-110819-FightingCybercrime.pdf, [last access: 30 April 2016 at 04:37 pm]

[58] Ibid Article 2

[59] Ibid Article 33(1)

[60] Official Gazette of the Common Market for Eastern and Southern Africa (COMESA) Vol. 16 No. 2 ,15 October 2011, available at: http://www.comesa.int/attachments/article/26/2011Gazette%20Vol.%2016.pdf, [last access: 30 April 01:54 am]

[61] Section 41 COMESA Model Cybercrime Bill, February 2013, available at: https://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf

[62] Ibid section 42

[63] Ibid section 43

[64] Ibid section 52

[65] SADC Model Law on Computer Crime and Cybercrime , Adopted on 02 March 2012, available at: https://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/TCY/2014/3021_model_law_study_v15.pdf, [last access: April 28 at 02:32]

[66] SADC Protocol on Mutual Legal Assistance in Criminal Matters, 3 October, 2002, available at: https://www.unodc.org/tldb/pdf/Malawi/MLW_MLA_Protocol.pdf, [last access: 27 April at 12:45 am]

[67] SADC Protocol on Extradition, 3 October, 2002, available at: http://www.sadc.int/documents-publications/show/Protocol_on_Extradiction.pdf, [last access: 12:53 am]

States are required to provide each other with "the widest possible measure of mutual legal assistance in criminal matters."[68]

In addition to the above cited Models that try to unify their efforts to create and maintain harmonized cybersecurity, another big step was among this row was conducted through the Octopus Conference in 2015. Key messages conveyed during the conference was about serious threats to human rights, democracy and the rule of law, as "cyberspace is not safe, crimes and violation of rights are not an exceptional cases and that offenders are not brought to justice."[69] During the conference again reinforced the reality that governments' ability to protect society against cybercrime and the rights of individuals thereto is limited.[70] They emphasize the need of more effective international cooperation and in this context that membership and use of the Budapest Convention on Cybercrime as a legal framework for international cooperation continue to increment. Capacity building will remain the most effective way of helping societies address the challenges of cybercrime and electronic evidence. It is a mainstream international policy. The protection of victims and their rights should be put at the forefront in order to ensure the effectiveness of the criminal justice system, as well as more cooperation amongst law enforcement, private sector and victim services is needed.

Chapter 3

The legal basis of State positive obligation for data protection and freedom of expression in digital world / the wider scope of Article 8 and Article 10 of ECHR

Among All CoE member states, Armenia also incorporated ECHR in its national law. States must act in accordance with the provisions of the Convention. The scope of Article 8 of the ECHR guarantees the protection of personal data in the light of the right to respect for private and family life.[71] The protection and retention of personal data clearly falls within the scope of private life as protected by Article 8 of the Convention. In its case law ECtHR examined many situations in which the issue of data protection arose, concerning interception of

[68] Ibid Article 2(1)

[69] Cooperation against Cybercrime, 17-19 June 2015, Council of Europe, Strasbourg, France, available at: http://www.coe.int/en/web/cybercrime/octopus2015

[70] https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680319026

[71] CoE, European Convention on Human Rights, CETS No. 005, 19, available at: http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/005, [last access: 2 May at 12:15pm]

communication[72], various forms of surveillance[73] and protection against storage of personal data by public authorities.[74]

Article 8

1. Everyone has the right to respect for his private and family life, his home and his correspondence.

2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

Indeed, the Court has stated that the protection of personal data is of fundamental importance to a person's enjoyment of his right to respect for private and family life.[75] The communications, telephone, e-mail and other forms of communication; informational privacy, including online information is within a scope of Private life.[76] In Flinkkilä and Others v. Finland the Court stated that the principle is that Article 8 protects personal information which individuals can legitimately expect should not be published without their consent[77]. But also in its case law the Court found that the monitoring of the applicant via GPS and the processing and use of the data obtained thereby amounted to an interference with his private life as protected by Article 8 § 1.[78]

Expansion of the Positive Obligations Doctrine under Article 8: **Basic principles in respect of data storage as set out in the Court's case-law.**

The European Convention on Human Rights refers to an obligation to respect human rights. According to Article 1 of the Convention "The High Contracting Parties shall secure to everyone within their jurisdiction the rights and freedoms defined in Section I of this Convention."[79] Normally these obligations are divided into negative and positive obligations. Negative obligation means that a state is compelled to abstain from interference in Convention guarantees. The positive obligations are additional to the negative obligations. Article 8 is essentially to protect the individual against arbitrary interference by the public authorities; there may be positive obligations inherent in an effective respect for private or family life[80]. "Positive

---

[72] Malone v. the United Kingdom, No. 8691/79, 2 August 1984
[73] Uzun v. Germany, No. 35623/05, 2 September 2010
[74] Marper v. the United Kingdom, Nos. 30562/04 and 30566/04, 4 December 2008
[75] S. and Marper v. the United Kingdom [GC], nos. 30562/04 and 30566/04, § 41, 4 December 2008
[76] Copland v. the United Kingdom, no. 62617/00, ECHR 2007-I
[77] Flinkkilä and Others v. Finland, no. 25576/04, § 75, 6 April 2010; Saaristo and Others v. Finland, no. 184/06, § 61, 12 October 2010
[78] In Uzun v. Germany, no. 35623/05, 2 September 2010
[79] ARTICLE 1, European Convention on Human Rights (ECHR), 4 November 1950, last access: http://www.echr.coe.int/Documents/Convention_ENG.pdf , [March 5 at 11:44pm]
[80] Airey v. Ireland, ECtHR, 9 October 1979, § 32, Series A no. 32

obligations" [81] mainly refers to a duty to protect individuals. State must take reasonable measures to protect individuals from infringements of their Convention rights by the other individuals, such as the relationships Internet user and those who provide access to a particular website. In other words, there is a positive obligation on the State to ensure an effective deterrent against grave acts to a person's personal data[82].

However, the concept of positive obligation of Article 8 was developed in *Marckx v Belgium*[83] .

The Court stated, in terms which have been repeated many times in later judgments, that:

"…As the Court stated in the *Belgian Linguistic* case, the object of the Article is 'essentially' that of protecting the individual from arbitrary interference by the public authorities. Nevertheless, it does not merely compel the State to abstain from such interference: in addition to this primarily negative undertaking, there may be positive obligations inherent in an effective 'respect' for family life". [84]

Positive obligation is imposed in circumstances where the State can "reasonably be expected to act so as to prevent or put an end to the alleged infringement of the applicant's rights."[85]In other words, State must ensure an effective deterrent against grave acts to a person's personal data[86].

The recent key case which stresses of the positive obligation of State connected an Internet-related complaint K.U. v. Finland. The teleological interpretation (aim and purpose of the Convention) widens the scope of Article 8. The obligation under the ECHR rests with the State as the Convention only indirectly guarantees human rights protection between individuals. But what are the protective measures that required from national authorities? What special concerns on the Internet must be addressed creating a framework that protects individuals from infringement by other individuals?

K.U. v. Finland (2008): Internet and the Right to Respect for Private Life under Article 8: Protection against Other Individuals. The recent key case which stresses of the positive obligation of State connected an Internet-related complaint K.U. v. Finland.[87] March 1999, on this day, an unknown person placed an advertisement on a dating site on the internet in the name of a 12 year old boy, K.U. The advertisement mentioned the age and year of birth of the boy. It also gave a detailed description of his physical characteristics and a link to his website. This included his picture, and his telephone number, which was correct save for one digit. It was claimed in the advertisement that he was looking for an intimate relationship with a boy of his

[81] A Mowbray The Development of Positive Obligations under the European Convention on Human Rights by the European Court of Human Rights (Hart, 2002) pp.225-227.
[82] August v. the United Kingdom (dec.), no. 36505/02, 21 January 2003
[83] (1979) 2 EHRR 330.
[84] *Belgian Linguistic (No 2)* (1968) 1 ECHR 252 para 7.
[85] *Fadeyeva v Russia,* Judgment of , 9 June 2005
[86] August v. the United Kingdom (dec.), no. 36505/02, 21 January 2003
[87] K.U. v. Finland, application no. 2872/02, § 43, 2 December 2008

age or older 'to show him the way'. The young applicant was subjected to an advertisement of a sexual nature. The problem was that the identity of the person who had placed the advertisement could not be obtained from the Internet provider. The legislation in place did not have any enforcement procedure to address such a situation. [88]

The positive obligations doctrine was brought forward in the Court's reasoning. As in the landmark case of X and Y v. the Netherlands (1985)[89] when the Court found that Article 8 was breached because domestic criminal law did not provide practical and effective protection of mentally ill girl who was sexually assaulted. In its judgment the court added another sentence to the now familiar formulation of the positive obligation:

"There may be positive obligations inherent in an effective respect for private or family life … These obligations may involve the adoption of measures designed to secure respect for private life even in the sphere of the relations of individuals between themselves".[90]

"While the choice of the means to secure compliance with Article 8 in the sphere of protection against acts of individuals is, in principle, within the State's margin of appreciation, effective deterrence against grave acts, where fundamental values and essential aspects of private life are at stake, requires efficient criminal-law provisions."[91] The positive obligations to secure respect for private life extend to the horizontal relations between individuals, and are not only applicable in the vertical relations between individuals and public authorities. The court also recalled its earlier case law, according to which in cases where fundamental values and essential aspects of private life are at stake, efficient criminal law provisions are required.[92]

In the K.U. case, the Court collected comparative international material on cybercrime. The Court used the material as evidence that the national authorities were aware of the problems related to the Internet. They address the challenge that the new technologies present, necessitating the adoption of international legal instruments to combat cybercrime. The Court referred in "International material" to the European Convention on Cybercrime[93].

The Court emphasized that it is nonetheless the task of the legislator to provide the framework for reconciling the various claims which compete for protection in this context. No such framework, however, was in place at the material time, with the result that Finland's positive obligation with respect to the applicant could not be discharged. National authorities had also acknowledged the failure and addressed the problem with a legislative amendment. The

[88] K.U. v. Finland, application no. 2872/02, § 43, 2 December 2008
[89] Barbulescu v Romania *([2016] ECHR 61)*
[90] Ibid
[91] K.U. v. Finland (2008), § 43
[92] K. U. v Finland, 43; the ECHR cited its judgments on the case of X and Y v the Netherlands, judgment of 26 March 1985, Series A no 91, §§ 23-24 and 27, and the case of August v United Kingdom (dec.), no 36505/02, 21 January 2003 and M.C. v Bulgaria, no 39272/98, § 150, ECHR 2003-XII.
[93] CETS 185, 23.11.2001. in force 1.7.2004

Government's argument was that the new legislation reflects the legislator's reaction to social development where an increased use – and at the same time abuse – of the Internet has required a redefinition of the limits of protection. The Court found that this was already the case at the time of the events in question. The K.U. case provides a start for criteria on protecting right to private life on the Internet.

As we have already realize K.U. v Finland is significant; because it requires Contracting States to ensure high quality IT systems to be in place in order to provide for the positive obligations of the protection of private life in relations between individuals themselves. In addition, the court also requires Contracting States to have practical and effective legal protection in place, including criminal sanctions, to provide for the protection of private life. This judgment requires governments and legislators to follow societal and technological developments, and to ensure that the legislation in force can provide effective protection. The court extended the principle of practical effectiveness of protection and its implication to require practical effectiveness of investigations to cover electronic evidence and information necessary to identify the perpetrator of the alleged offence.[94]

Freedom of expression*;*

The right of freedom of expression, it is protected by many fundamental international instruments.

Accordingly, Article 19 of the Universal Declaration of Human Rights says:

"Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers."

This right is further specified and made legally binding in Article 19 of the International Covenant on Civil and Political Rights and in Article 10 of the European Convention on Human Rights. Consequently, Freedom of expression, protected by Article 10 § 1 constitutes an essential basis of a democratic society[95] and the limitations on that freedom foreseen in Article 10 § 2 are interpreted strictly.

Freedom of expression is guaranteed by Article 10 of the Convention in the following terms:

"1. Everyone has the right to freedom of expression. This right shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers. This Article shall not prevent States from requiring the licensing of broadcasting, television or cinema enterprises.

---

[94] K.U. v Finland, no. 2872/02, 2 December 2008; Article JUDGMENT IN THE CASE OF K.U. V FINLAND By Tuomas Pöysti, availabe at: http://sas-space.sas.ac.uk/5452/1/1855-2575-1-SM.pdf

[95] Handyside v. the United Kingdom, application no. 5493/72, 7 December 1976, Series A no. 24

2. The exercise of these freedoms, since it carries with it duties and responsibilities, may be subject to such formalities, conditions, restrictions or penalties as are prescribed by law and are necessary in a democratic society, in the interests of national security, territorial integrity or public safety, for the prevention of disorder or crime, for the protection of health or morals, for the protection of the reputation or rights of others, for preventing the disclosure of information received in confidence, or for maintaining the authority and impartiality of the judiciary."[96]

The Court's general principles concerning freedom of expression apply to the Internet

.Interpretation of the Convention "in the light of present-day conditions" must take into account the specific nature of the Internet as a "modern means of imparting information."[97] In its recent case law Court stated the Internet is a tool which gives citizens an opportunity to exercise their right to "freedom of information"[98]. The Convention, thus, has an increasingly important role to play in this area in series of recent judgments[99] which clearly illustrate the awareness by the European Court of the utmost importance of freedom of expression and information in a democratic society. Internet publications fall within the scope of Article 10, nevertheless it sets out certain restrictions on freedom of expression on the Internet. The Court also recognized explicitly the right of individuals to *access the internet*. The Court asserted that the internet has now become one of the principal means of exercising the right to freedom of expression and information[100] in its ruling against the blocking of online content (on Google Sites).

Nevertheless, Article 10 as mentioned above does not guarantee unlimited freedom of expression, but the scope of Article 10 covers criticism or satire as court deems that without these "democratic society" cannot exist. Those are the demands of pluralism and tolerance. By contrast, offensive and injurious speech on the Internet that goes beyond the satirical and defamatory in nature leads the Court to reject an application.[101] Domestic courts must give relevant and sufficient reasons for the justification a judgment finding that someone has committed defamation on the Internet which Court will have to test. Indeed, hate speech does not benefit from the protection of Article 10 of the Convention[102] as in Perrin v. the United Kingdom the Court rejected the applicant's complaint under Article 10 of the Convention as inadmissible (manifestly ill-founded). The case is about a Fernch national based in UK who was

[96] ARTICLE 10, European Convention on Human Rights (ECHR), 4 November 1950, available at: http://www.echr.coe.int/Documents/Convention_ENG.pdf, [last access: May 1 at 8:17pm]
[97] Internet: case-law of the European Court of Human Rights Updated: June 2015; available at www.echr.coe.int (Case-Law – Case-Law Analysis – Case-law research reports).
[98] ECtHR 18 December 2012, Case No. 3111/10, Ahmed Yildirim v. Turkey.
[99]In 12 judgments it found no violation of that right. In other cases it relied on Article 10 in order to justify that there had not been a violation of Article 8 in cases of alleged privacy breaching or defamatory media reporting. Available at: http://www.echr.coe.int/Documents/Annual_Report_2014_ENG.pdf.
[100] ECtHR 18 December 2012, Case No. 3111/10, Ahmed Yildirim v. Turkey. See also ECtHR 10 March 2009, Case Nos. 3002/03 and 23676/03, Times Newspapers Ltd. (n° 1-2) v. UK.
[101] Bartnik v. Poland (dec.), no. 53628/10, 11 March 2014
[102] Gündüz v. Turkey, no. 35071/97, § 41, ECHR 2003-XI

operating a United States-based Internet company with sexually explicit content for publishing obscene articles on Internet. In these circumstances Court found that criminal conviction considered necessary and proper for a democratic society and was not disproportionate.

ECHR Case law: Internet and defamation, threats and insults

Delfi AS v. Estonia [103] was the first case in which the Court had been called upon to examine a complaint about liability for user-generated comments on an Internet news portal. The Court notes at the outset that user-generated expressive activity on the Internet provides an unprecedented platform for the exercise of freedom of expression. That is undisputed and has been recognized by the Court on previous occasions[104]. The applicant runs a news portal Estonia complained that its liability by the national courts for the offensive comments posted in online news articles about a ferry company by its readers. They were defamatory because of vulgar, degraded human dignity and contained threats. The applicant company removed the offensive comments after six weeks of their publication. The Court held that there had been no violation of Article 10 of the Convention, finding that the Estonian courts' finding of liability against the applicant company had been a justified and proportionate restriction on the portal's freedom of expression, in particular, because: the comments in question had been extreme, had been posted in reaction to an article and the steps taken in order to remove the offensive comments without delay had been insufficient; and the fine posted by no means been excessive as it is largest Internet portal in Estonia.

The protection of freedom of expression under Article 10 against the right of offended parties to protect their reputation, which, as an aspect of their private life, is protected by Article 8 is a matter of recent considerations. In such cases the Court verifies whether the national authorities have struck a fair balance between these two rights, which it considers to be of equal importance. Court these cases call for "a balancing exercise between the right to freedom of expression and the right to respect for private life"[105]. The outcome of the application should not, in principle, vary according to whether it was lodged with the Court under Article 8 of the Convention by the person who was the subject of the offending article or under Article 10 of the Convention by the publisher who published it. Indeed, these rights "deserve equal respect" and the margin of appreciation should in principle be the same in both cases.

Positive Obligation- In the judgment Editorial Board of Pravoye Delo and Shtekel v. Ukraine[106] the Court, for the first time, acknowledged that Article 10 of the Convention had to be

[103] Delfi AS v. Estonia, application no. 64569/09, 16 June 2015 (Grand Chamber)
[104] Ahmet Yıldırım v. Turkey, no. 3111/10, § 48, ECHR 2012, and Times Newspapers Ltd (nos. 1 and 2) v. the United Kingdom, nos. 3002/03 and 23676/03, § 27, ECHR 2009
[105] Axel Springer AG v. Germany, application no. 39954/08, ECtHR, 7 February 2012
[106] no. 33014/05, 5 May 2011

interpreted as imposing on States a positive obligation to create an appropriate regulatory framework to ensure effective protection of journalists' freedom of expression on the Internet. The recognition by the European Court of a *horizontal effect* of Article 10, assessing interferences with the right to freedom of expression by private persons or corporate organisations, and of the *positive obligations* for member states to protect and effectively create an environment for guaranteeing the right to freedom of expression has further extended the scope of that right. Positive obligations of States and protection of individuals' rights in internet: first of refers to the integrity of vulnerable individuals, in particular, children and minors. In the Internet context the notion "vulnerable" court has taken into consideration the impact data accessible online can have on children[107] As cited above in Perrin Case, a criminal conviction for pornographic and scatological photographs on the Internet, accessible free of charge on a preview page (without any age checks) may fall under the State's obligation to protect morals and the rights of others. The State is at fault if it does not protect or seek to protect young people, a vulnerable category, in its legislation.[108]

Chapter 4

Cybercrime in Armenia: The effectiveness of RA Criminal Code and Criminal Procedural Code

According to Article 6 of RA Constitution:

"…International treaties shall enter into force only after being ratified or approved. International treaties are an integral part of the legal system of the Republic of Armenia. If ratified international treaties define norms other than those provided for by laws, such norms shall apply…"[109]

The Convention on Cybercrime – the main international treaty ratified by Armenia in 2006- requires states parties to make illegal certain acts provided by the Convention criminalize under their national law. Its Additional Protocol requires states parties to criminalize the dissemination of racist and xenophobic material (hate speech). After ratification Armenia passed to another level of working and elaborating the efforts to fight against cybercrimes. New legal acts were

[107] Mouvement raëlien suisse v. Switzerland [GC], application no.16354/06, ECtHR, 13 July 2012
[108] Application no. 5446/03, by Stephane Laurent PERRIN against the United Kingdom
[109] The Constitution of the Republic of Armenia, adopted on 5 July, 1995, The constitutional amendments were adopted on 27 November, 2005,by a referendum, available at: http://concourt.am/english/constitutions/index.htm, [last access: May 1 at 09:47 pm]

developed and introduced, working and educational visits to the different European countries organized in order to investigate their best practices.

Chapter 24 of RA Criminal code is devoted to crimes against computer information security. The consecutive 7 articles apply to the cybercrimes: Article 251-Access (penetration) into computer information system without permission, Article 252 -Change in computer information. Article 253 -Computer sabotage. Article 254- Illegal appropriation of computer data. Article 255-Manufacture or sale of special devices for illegal penetration into a computer system or network. Article 256- Manufacture, use and dissemination of hazardous software. Article 257- Breach of rules for operation of a computer system or network.[110] Also the following articles of RA Criminal Code which is not within a scope of chapter 24, prescribes crimes via using computer information systems: Article 181-Theft committed by means of computer; Article 144- Illegal collecting, keeping, use and dissemination of information pertaining to personal or family life; Article 137- Threat to murder, to inflict heavy damage to one's health or to destroy property; Article 140- Forced violent sexual acts; Article 166-Involving a child into antisocial activity; Article 263-Illegal dissemination of pornographic materials or items; Article 182- Extortion.[111]

In Armenia the criminal investigations of the crimes against computer security are implemented by the criminal investigation units of the RA Police is established in 2005.[112] The division to combat against cybercrimes further supplemented by officer positions in order to provide every day implementation of 24/7 contact point obligation under the Cybercrime Convention.[113]

Cybercrime case study in Armenia:

In Armenia the first scandalous criminal case on the grounds of cybercrime was in 2013 against Russian citizen Georgi Avanesov, who was sentenced to 4 years in prison. According to this case, being in Armenia in 2009-2010, Avanesov succeeded to break the Kaspersky anti-virus system and to infect 29 million computers worldwide having a chance to illegally dispose the stored data in them by disseminating malicious programs through special bugs.[114] After gaining the control of the Bredolab botnet he was arrested. Avanesov was convicted of using his botnet to carry out distributed Denial of Service (DDoS) attacks on multiple computer systems owned by private individuals and organizations. It international media paid high attention to this case and reported that Avanesov was earning up to £80,000 a month from the botnet.[115]

---

[110] Criminal Code of The Republic of Armenia, 18.04.2003, available at: http://www.arlis.am/, [last seen: May 2 11:11 pm]

[111] Ibid

[112] http://www.jnews.am/en/cybercrime-in-Armenia

[113] http://www.police.am/en/home.html

[114] ԵՆՔԴ/0144/01/11, www.datalex.am

[115] http://www.ibtimes.co.uk/bredolab-botnet-jailed-armenia-avanesov-345021

Avanesov's case is a special one, as it was the first case in the legal practice of Armenia, which of course created challenges, and that lack of experience was the reason that he was charged under 4 different articles of the 24 chapter of Criminal Code of RA. As a result of the trial Avanesov was found guilty according to one article. He has been sentenced for offenses under Part 3 of the Article 253 of the Armenia's Criminal Code.

Article 253. Computer sabotage.

"1. Obliteration (sabotage) of computer data or software, isolation or making it unusable, spoilage of computer equipment or destruction of the computer system, network or on storage media, is punished with a fine in the amount of 300 to 500 minimal salaries, or with correctional labor for the term of up to 1 year, or with arrest for the term of 1-3, or with imprisonment for the term of up to 2 years…"[116]

However in some articles on cybercrime of RA Criminal Code do not meet the standard of legal certainty. This ambiguity will lead to the confusion in the legal practice and wrong criminal descriptions as a consequence can emerge. Particularly "There is no norm pointing out the meaning of the concept "serious consequences". For example, in the case of property crimes there are options: considerable, large, in particularly large amount. But in this case there is no such kind of certainty and the term "serious consequence" is strictly evaluative and discretionary in some norms of the Criminal Code.[117]

Defamation and insult conducted by internet; the gap of Armenian legislation

Parliamentary Assembly of Council of Europe invited states to repeal or amend criminal defamation provisions in 2007.[118] Previously, defamation and insult were covered and regulated through the Articles 135 and 136 of Criminal Code of RA adopted in 18 April, 2003.

In accordance with the Council of Europe resolution "Towards decriminalization of defamation" the Republic of Armenia decriminalized defamation and libel[119]and consequently abolished criminal liability for defamatory statements.

Considering current regulation of Armenia with regard defamation and insult consulted by means of internet we can conclude that effective judicial mechanism currently is not in place.

---

[116] RA Criminal Code, adopted in on April 18, 2003; available at http://www.arlis.am/DocumentView.aspx?DocID=102896

[117] http://www.jnews.am/en/cybercrime-in-Armenia?page=1&quicktabs_4=0

[118] Recommendation 1814 (2007) and Resolution 1577 (2007) of the Parliamentary Assembly "Towards decriminalization of defamation", available at http://www.assembly.coe.int/nw/xml/XRef/X2H-Xref-ViewHTML.asp?FileID=11684&Lang=EN, [last access: 25 April 2016 at 06:07 pm].

[119] The Republic of Armenia Law on Making Amendments to the Republic of Armenia Criminal Code, adopted on 18 May, 2010, available at http://www.arlis.am, [last access: 4 April 2016 at 07:57 pm].

In particular, the article 1087.1 was included in RA Civil Code from May of 2010 which regulates defamation and insult by the "Procedure for and Conditions of Compensation for the Damage Caused to Honor, Dignity and Business Reputation "[120]

According to part 3 of the same article slander is:

"Within the meaning of this Code, slander shall be deemed as public communication of factual data (statement of fact) relating to a person, which do not correspond to the reality and disgrace the honor, dignity or business reputation thereof"[121]

Under the provisions of the same article the a person shall have the right to require, under a judicial procedure, from the person having insulted or slandered him or her to compensate the damage only if the person who caused insult or slander is known.

The judicial protection enshrined in the article 1087.1 also extends to the part 5 of article 22 of RA Civil Code:

"The damage caused to a person upon illegal use of his or her name shall be subject to compensation in accordance with this Code.

In case of distorting or using the name of a citizen in a way or in a form that affects his or her honor, dignity or business reputation, the rules provided for by Article 1087.1 of this Code shall apply".

Those protection enshrined in abovementioned articles are effective if the identity of offender is discovered. But the remaining cases where the gathering, preserving and using of such information conducted through by anonymous users of computer systems or through the internet, the protection enshrined of Civil Code within previously discussed articles does not operate and protect adequately. In this situation even if the use of personal data can be qualifies as "defamation", the legislative regulation cannot be considered sufficiently effective, because the lack of opportunity to bring a civil lawsuit against the offender.

Even if the article prescribes criminal liability; nevertheless some concepts in this article also can be defined as not effective protection in case of use of personal data and information related to the person. Moreover, as already mentioned above if the offence conducted through the internet where the process of discovering a criminal itself very risky.

Laws must provide effective protection in regard to the dissemination of offensive statements which become the most common problem in line with the development of the Internet and the Civil Code provisions must be stipulated in a way that will preclude the exemption of liability in favor of defamatory speech. The existence of such provisions may pose a threat to protection of

[120] The Republic of Armenia Law on Making Amendments to the Republic of Armenia Civil Code, adopted on 18 May, 2010, available at http://www.arlis.am,

[121] RA Civil Code, adopted May 5, 1998, available at: http://www.arlis.am/, [last access: 1 May 03:10 pm]

right to respect for private and family life of Article 8 of the European Convention on Human Rights and is likely to be determined to be a violation.

Personal Data protection: The guarantees of Article 144 of RA Criminal Code with regard Article 8 ECHR

Article 144 of RA Criminal Code: Illegal collecting, keeping, use and dissemination of information pertaining to personal or family life reads as follows:

"Information which is considered to be a personal or family secret used without one's consent or dissemination by public speeches, publicly demonstrated works or through mass media, or collecting or keeping, unless this is envisaged by law, is punished with a fine in the amount of 200 to 500 minimal salaries, or correctional labor for up to 1 year, or with arrest for the term of 1 to 2 months"[122]

" Although the Republic of Armenia is not a member state of the European Union, the Directive on Data Protection in force constitutes a sound legal parameter to which refer for evaluating any legislative effort in this area. Despite the Republic of Armenia is not legally bound by Directive 95/46, there is a reasonable expectation that such data, which of course amount to "personal data" benefit from a special protection compared to other types of information. As a contracting state, in fact, it must provide protection of an appropriate degree to personal data as an essential part of the right to private life enshrined to Article 8 of the European Convention on Human Right."[123]

The Directive 2002/58/EC is about the confidentiality of personal data and electronic communication, which, above all, enshrined by international conventions like ECHR.

In particular Article 8 of the Convention underlines that new digital technologies implies an obligation the protection of the confidentiality of personal life and personal data.

Consequently, Directive 2002/58/EC in its Article 5 make an obligation for Member States to have a national legislation in place which will ensure the confidentiality of communications and the related traffic data by means of a public communications network and publicly available electronic communications services.[124]

The protection of personal data is a state obligation with providing such technical and organizational measures that will provide a safe environment of protection of personal data, from illegal or random deletion or loss, from unauthorized modification, use, access or disclosure.

---

[122] http://www.arlis.am/DocumentView.aspx?DocID=102896

[123]LEGAL ANALYSIS OF DRAFT AMENDMENTS TO THE CIVIL CODE OF THE REPUBLIC OF ARMENIA, Commissioned by the Office of the OSCE Representative on Freedom of the Media from Oreste Pollicino, Associate Professor of Media Law, Bocconi University, Milan, March 2014 ; available at: http://www.osce.org/fom/116911?download=true, [last access: 1 May 02:24 pm]

[124] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32002L0058

This is the reason why it is worthy, although Armenia is not member of the EU, to look at the legislation in question also in light of the legal framework adopted herein.[125]

Those data become easily available by the proliferated use of internet, as many of us register those data in internet for different purposes. This is the main reason why the majority of the countries despite the separate regulation of personal data protection define additional clause in Criminal Code which prevent the theft of ID. In Armenia in 2015 adopted Law of the Republic of Armenia on the Protection of Personal Data.[126]

Thus, in order to avoid widespread violations, sever consecutive steps can be taken for the improvement of protection and creation more sophisticated standards:

- Comparing with Article part 9 of Article 152 of Civil Code of Russian Federation[127] which reads that "If the person, who has spread the information, discrediting the honor, dignity or business reputation of the citizen, cannot be identified, the citizen shall have the right to turn to the court with the demand that it recognize the spread information as not corresponding to reality." This refer to the situation when the respondent in the Court does not really obvious and in this situation the legislator enshrines with effective measure to demand protection from Court by simply be recognizing erroneous information. Such kind of regulation has an urgent importance because the easy access and search the content of online-posted materials in internet, very often it leads to the false statement or review damaged the reputation of individuals. That is the appropriate amendments should be conducted in RA Civil Code, in order to enable individual to protect their reputation in that particular situation. This indeed can act as a deterrent and preventive measure and can be a unique tool for the protection of honor and dignity.

- Moreover, it will be very important to prescribe new separate clause named as: "illegal use personal data" of crime within RA Criminal Code the article must impose a liability for illegal obtaining, maintaining, processing and using personal data. It must have a differentiated approach having regarded the effect, damage.

- To redistribute Crimes against computer information security included in Chapter 24 of RA Criminal Code to the Initiation of a criminal case based on the complaint of the injured person prescribed by the article 183 RA Criminal Procedure Code

- To define a damage in all articles as "significant damage" having in mind damage posed the legitimate interest and rights of person

---

[125] Even though it is not binding legislation to Armenia, Directive 2000/31/EC adopted by the European Union establishes common principles governing liability of Internet service providers and it could be considered to be a proper source of inspiration

[126] http://www.parliament.am/legislation.php?sel=show&ID=5275

[127] Civil Code of Russian Federation, Part 1, adopted on 21 October, 1994, available at http://www.gk-rf.ru, [last access: 1 May 2016 at 7:30 pm]

- To prescribe to the second part of particular articles stricter liability, having regard consequences, in particular already envisaged concepts of "heavy consequences" or "financial" or "large loss" in RA Criminal Code.
- To ratify another international treaty which will enhance the protection and will promote the standardization and effective protection against cybercrime in Armenia
- To invite international experts to make trainings among our specialist.
- To invest in research, technology and capacity building. In order to enclose more knowledgeable cyber-security people in the public sector, in that regard to establish R&D center for developing cybersecurity standards, have certified agencies which will incorporate best practices and can serve guidelines.
- Comparing to other states of South Caucasus Armenia is not a member of the FIRST (Forum of Incident Response and Security Teams) organization. FIRST arranges conferences and takes part in development activities for CERTs (technical standards to enhance cybersecurity). That is why the Armenian CERT web page presents outdated information. Armenia must make it a priority to strengthen and develop their CERT's capabilities. The existence of an operational national CERT could be helpful for countering cybercrime.
- Defining legal frameworks that require amendments, updates or changes: As in many countries Armenia also can add to its substantive criminal law and procedural law, Cybercrime legislation, which will touch upon the issues related to international cooperation, electronic evidence and the liability of an Internet Service Provider (ISP).
- To extend regional approaches to cybersecurity as it does effect in many sub regional areas discussed above, participate in international cyber exercises, because of the need to strengthen to police and prosecution and initiate concrete legislation amendments.
- Armenia does not have a multi-stakeholder approach, which will allow all national stakeholders from the public and private sector to involve in the development, implementation and enforcement of a cybersecurity strategy
- Crimes do not always rely upon the lack of technical protection, but the lack of knowledge and awareness of victims. "Phishing" is a sound example for this. The education of Internet users reduces the number of potential targets. Users can be educated through public campaigns, lessons in schools, libraries, IT centers and universities.
- The cryptography[128]as a protection tool is a large scale phenomenon in the western world. The incorporation of this method can help improve data protection. If the person or organization

[128] Cryptography is a method of storing and transmitting data in a particular form so that only those for whom it is intended can read and process it , available at: http://searchsoftwarequality.techtarget.com/definition/cryptography

storing information uses proper protection measures, cryptographic protection can be more efficient than any physical protection.[129]

- Armenia can create cyber defense groups under the law enforcement agencies, which will play an informatory role about existing cyber-threats. .
- National judicial administrations and legal educational institutions should include comprehensive criteria on computer-related crime in their teaching schedules and enhance their suitability in a changing world and make them competent.

Conclusion

Within the ambit of this paper we have already discussed the essence of cybercrime as the new and unprecedented threat to the nowadays world which, undoubtedly, requires effective combat efforts. The new elaborated types of cybercrimes, which know no borders, can infect simply the targets merely within seconds, by hacking, phishing, delivering spams, viruses, worms, etc. The obtaining of identity information through those techniques brought the reality that the protection of ID becomes more sensitive than ever before and implies high risks to the individuals. It is obvious that collaborate mechanisms within international level is a matter of priority for effective fight against these crimes which increments proportionally with the proliferation and dependence of our day to day activities from internet. In this effect many international Conventions and Directions adopted for the proper response respectively to the protection of personal data and regulation of cybercrime.

Furthermore, the crimes conducted via internet challenged the basic human rights of citizens inside States which lead to the new approaches of current changing environments that goes beyond traditional interpretation of ECHR, but extended alongside to the negative obligation to the positive obligation, which requires states to make an such an environment through the adequate legislation and sophisticated mechanisms. It is a mere fact that every state's obligation is to elaborate their national legislation, technical support or input other effective mechanisms for the whole pocket of combat as it is an effective cybersecurity is the important cornerstone to ensure safe society, where basic human rights are protected, particularly Private Life and Freedom of Expression enshrined in ECHR.

As we have already discussed the international and regional initiatives on the way of detect existing challenges and flows envisaged in the framework of this paper, indeed are adequate initiatives and can serve as valuable guidance and can have an enormous role within a

[129] Schneier, "Applied Cryptography", page 185, 1996

harmonization of cybercrime laws and overall for holistic approach. In order to succeed many regions attempted to face these current threats with the aim of comprehensive approach and facilitating current Risk.

Furthermore, for states, particularly for Armenia to have a united national strategy in this sphere at State level is a "must" which will encompass enhance the cybersecurity profile in Armenia. The following steps as the establishment educational efficient system, amendment of Criminal Code for the necessity of legal specification, the creation of the analytical and educational centers can be very useful. Nevertheless, as the main impediment for this process is existing differences between national laws in this regard it is important to strengthen a comprehensive international collaboration which will facilitate effective cooperation, the widest extent possible, as the unique character of cybercrime requires a collaboration of law-enforcement and judicial authorities. These steps must be taken in order to have in place more holistic, sophisticated and safe environment, which will reduces the threats for the citizens to be exposed by the violations of their basic rights embedded in International Conventions and will lead effective implementation of state positive obligation towards its individuals.

Bibliography

Legal Documents:

1. The RA Constitution adopted July 5, 1995
2. Criminal Code of The Republic of Armenia adopted April 18, 2003
3. RA Civil Code, adopted May 5, 1998
4. Directive on attacks against information systems, Strasbourg, adopted 4 July 2013
5. Directive 95/46/EC of the European Parliament and of the Council of, adopted 24 October 1995
6. Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002
7. Directive 2000/31/EC adopted by the European Union, adopted 8 June 2000
8. T-CY Guidance Notes , adopted by the 8th, 9th and 12th Plenary of the T-CY, 8 December 2014
9. Convention on Cybercrime, CETS No. 185, Budapest, adopted 23 November 2001
10. CoE, European Convention on Human Rights, CETS No. 005, adopted 4 December 1950.
11. T-CY Guidance Note #2, Provisions of Budapest Convention covering botnets, Adopted by the T-CY at its 9th Plenary, June 5, Strasburg, 2013,
12. A/RES/45/121, adopted by the UN General Assembly on 14 December 1990

13. A/RES/55/63, adopted by the UN General Assembly on12 December 2000
14. A/RES/57/239, adopted by the UN General Assembly on 31 January 2003
15. A/RES/58/199, adopted by the UN General Assembly on 30 January 2004
16. Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Council of Europe, CETS No. 108, adopted 1981
17. United Nations Manual on the Prevention and Control of Computer-Related Crime, adopted 1994
18. African Union (AU) Convention on Cyber Security and Personal Data Protection, EX.CL/846(XXV) adopted 27th June 2014
19. African Union: Draft Report, adopted March 2008
20. ECOWAS Directive C/DIR.1/08/11 on Fighting Cybercrime, adopted August 2011
21. SADC Model Law on Computer Crime and Cybercrime , adopted 02 March 2012
22. SADC Protocol on Mutual Legal Assistance in Criminal Matters, adopted 3 October, 2002
23. SADC Protocol on Extradition, adopted 3 October, 2002
24. Council of Europe Recommendation 1814, adopted 26 June 2007
25. Council of Europe Resolution 1577, adopted 4 October 2007

Publications:

1. Sofaer/Goodman- The Transnational Dimension of Cyber Crime and Terrorism, 2001
2. UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue, dated 10 August 2011, UN Document A/66/290
3. Yves Poullet, "Internet of the future: achieving transparency, pluralism and democracy" November 2009
4. Scene of the Cybercrime, Second Edition, Littlejohn Shinder and Michael Cross, 2008
5. 10th UN Congress on the Prevention of Crime and the Treatment of Offenders, 2000, A/CONF.187/10
6. Goodman "Why the Policy don't care about Computer Crime, Harvard Journal of Law & Technology", 2007
7. Goodman/Brenner, The Emerging Consensus on Criminal Conduct in Cyberspace, UCLA Journal of Law, 2002
8. Hayden, Cybercrime's impact on Information security, Cybercrime and Security, ITU 2012
9. Hale, Cybercrime: Facts & Figures Concerning this Global Dilemma, 2002

10. Aghatise E. Joseph, research report, June 28, 2006,
11. Walden, Computer Crimes and Digital Investigations, 2006
12. Wilson, Botnets, Cybercrime, and Cyberterrorism: Vulnerabilities and Policy Issues for Congress, 2007
13. Jakobsson, The Human Factor in Phishing, 2007
14. The Crimeware Landscape: Malware, Phishing, Identity Theft and Beyond, October 2006
15. ITU Survey on Anti-Spam Legislation Worldwide, 2005
16. Bryan Harris/Eli Konikoff /Phillip Petersen, Breaking the DDoS Attack Chain, CMU-ISR-MITS-2, 2013
17. California Pacific School of Law. Gonzaga Journal of International Law. Volume 1, 1997-1998
18. ITU Global Cybersecurity Agenda / High-Level Experts Group, Global Strategic Report, 2008
19. Declaration Synergies and Responses: Strategic Alliances in Crime Prevention and Criminal Justice, 2005
20. LMM(02)17 – Report to Law Ministers, 2002
21. Cybercrime Model Laws, Discussion paper prepared for the Cybercrime Convention Committee (T-CY), 23 December 2014
22. Schjolberg/Hubbard, "Harmonizing National Legal Approaches on Cybercrime", 2005
23. Uchenna Jerome Orji, "Examining Missing Cybersecurity Governance Mechanisms in the African Union Convention on Cybersecurity and Personal Data Protection", Computer Law Review International, October, 2014
24. A Mowbray, "The Development of Positive Obligations under the European Convention on Human Rights by the European Court of Human Rights", Hart, 2002
25. Judgement in the case of K.U V Finland by Tuomas Pöysti, 2009
26. Internet: case-law of the European Court of Human Rights Updated: June 2015
27. Legal Analysis of Draft Amendments to The Civil Code of the Republic of Armenia, Commissioned by the Office of the OSCE Representative on Freedom of the Media from Oreste Pollicino, Associate Professor of Media Law, Bocconi University, Milan, March 2014
28. Schneier, Applied Cryptography, 1996
29. Annual Report, European Court of Human Rights, adopted 2014
30. HIPCAR Cybercrime/e-Crimes: Model Policy Guidelines & Legislative Texts, ITU 2012

Case Study:

1. Malone v. the United Kingdom, application no. 8691/79, ECHR, 2 August 1984
2. Uzun v. Germany, application no. 35623/05, ECHR, 2 September 2010
3. Marper v. the United Kingdom, Nos. 30562/04 and 30566/04, 4 December 2008
4. S. and Marper v. the United Kingdom application no. 30562/04 and 30566/04, ECHR, 4 December 2008
5. Copland v. the United Kingdom, application no. 62617/00, ECHR, 3 April 2007
6. Flinkkilä and Others v. Finland, application no. 25576/04, ECHR 6 April 2010
7. Saaristo and Others v. Finland, application no. 184/06, ECtHR 12 October 2010
8. Airey v. Ireland, application no. 6289/73, ECtHR, 9 October 1979
9. August v. the United Kingdom , application no. 36505/02, ECtHR , 21 January 2003
10. Marckx v. Belgium, application no. 6833/74, ECtHR , 13 June 1979
11. Fadeyeva v Russia, application no. 68443/01, ECtHR , 9 June 2005
12. August v. the United Kingdom , application no. 36505/02, ECHR , 21 January 2003
13. K.U. v. Finland, application no. 2872/02, ECHR, 2 December 2008
14. Barbulescu v Romania, application no. 61496/08, ECHR, 12 January 2016
15. X and Y v the Netherlands, application no. 8978/80, ECtHR, 26 March 1985
16. August v United Kingdom , application no 36505/02, ECtHR, 21 January 2003
17. M.C. v Bulgaria, application no. 39272/98, ECHR, 4 December 2003
18. Handyside v. the United Kingdom, application no. 5493/72, ECtHR, 7 December 1976
19. Ahmed Yildirim v. Turkey, application no. 3111/10, ECtHR, 18 December 2012
20. Bartnik v. Poland, application no. 53628/10, ECtHR , 11 March 2014
21. Gündüz v. Turkey, application no. 35071/97, ECtHR, 14 June 2004
22. Delfi AS v. Estonia, application no. 64569/09, ECtHR, 16 June 2015
23. Times Newspapers Ltd (nos. 1 and 2) v. the United Kingdom, application no. 3002/03 and 23676/03, ECHR, 10 March 2009
24. Axel Springer AG v. Germany, application no. 39954/08, ECtHR, 7 February 2012
25. Mouvement raëlien suisse v. Switzerland, application no.16354/06, ECtHR, 13 July 2012
26. Stephane Laurent PERRIN v. the United Kingdom, application no. 5446/03, ECtHR, 3 February 2003
27. ԵԱՔԴ/0144/01/11

Conferences:

1. United Nations Conference on Trade and Development, Information Economy Report 2005
2. Octopus Conference 2015 , Cooperation against Cybercrime, 17-19 June 2015, Council of Europe, Strasbourg, France

Web Sources:

1. www.defenselink.mil/transcripts/transcript.aspx?transcriptid=3996
2. http://searchsecurity.techtarget.com/definition/cybercrime
3. Computer Crime Research Center
4. www.netadmintools.com/part215.htm
5. http://us.norton.com/cybercrime-trojansspyware
6. http://vx.netlux.org/lib/ajm01.htm
7. http://www.itu.int/en/Pages/default.aspx
8. http://www.itu.int/en/ITU-D/Projects/ITU-EC-ACP/Pages/default.aspx
9. http://www.itu.int/en/ITU-D/Projects/ITU-EC-ACP/HIPCAR/Documents/FINAL%20DOCUMENTS/ENGLISH%20DOCS/e-transactions_mpg.pdf
10. http://www.jnews.am/en/cybercrime-in-Armenia
11. http://www.police.am/en/home.html
12. http://www.ibtimes.co.uk/bredolab-botnet-jailed-armenia-avanesov-345021
13. http://www.arlis.am/
14. http://www.parliament.am/
15. http://searchsoftwarequality.techtarget.com/definition/cryptography
16. www.datalex.am