Preparatory Colloquium
24-27 April 2013, Moscow (Russia)
Section II: Information Society and Penal Law

RUSSIAN NATIONAL REPORT*

Tatiana TROPINA*

A. Introduction

The recent growth of information technologies in Russia has brought all the possibilities and opportunities provided by global character and easiness of use of the new technologies for development of the society. However, at the same time it has also given the new opportunities for criminals utilizing the same advantages of these technologies. On the one hand, the growing number of Internet-users in Russia speeds up communications in everyday life and for commercial purposes, lowers the costs of doing business, increases the availability of information for educational purposes, and facilitates the development of such services as e-government[1]. On the other hand, with the creation of new opportunities for economic and social development, the spread of the new technologies in Russia has changed the criminal landscape and generated the challenges for government and society with regard to the use of these instruments for criminal purposes. With the growth of Internet users from 47 million to the middle of 2009[2] to 70 million in 2012[3], the growing problem of cybercrime in the last three years forced Russian legislators to react to the challenge of cybercrime by, firstly, amending the legislation in this area, and, secondly, proposing cybersecurity treaties on the international level[4].

The aim of this report is to analyse Russian legislation in the area of cybercrime with regard to the AIDP Questionnaire and international standards. It should be noted, however, that Russia is not a party of any international or regional agreement which has the standards provided by the AIDP Questionnaire (such as, for example, standards for criminalisation of CIA offences: illegal access, data and system interference, misuse of devices). It does not mean that Russian legislation is unable to address the threat of cybercrime effectively. However, some of the existing legal provisions are only partially compatible (or not compatible at all) with such instruments as, for example, Council of Europe Convention on Cybercrime.

---

* Important notice: this text is the last original version of the national report sent by the author. The Review has not assured any editorial revision of it.

* *Dr. Tatiana Tropina, Senior Researcher, Max-Planck Institute for Foreign and International Criminal Law*.

1 See e.g. *Dobrolyubova, Y.* Introducing Elements of E-Government in Russia: Achievements, Lessons Learnt, an Possible Prospects. Presentation at UNDESA Expert Group Meeting *E-Government and Public Private Partnerships: Towards Better Public Service Delivery and Implementation of the MDGs.* Geneva, May 21-22, (2009)

2 *Evplanov, A.* Runet: vne krisisa. Polzovateli Interneta v Rossii prirastut na tret. Rossiyskaya Gazeta, 19 May, 2009 // available at: http://www.rg.ru/2009/05/19/internet.html

3 Kolichestvo polzivataley Interneta v Rossii. 25.11.2012. Available at: http://www.bizhit.ru/index/users_count/0-151

4 See: Convention on international information security (concept), available at: http://www.mid.ru/bdomp/ns-osndoc.nsf/1e5f0de28fe77fdcc32575d900298676/7b17ead7244e2064c3257925003bcbcc!OpenDocument; Russia and China propose UN General Assembly Resolution on "Information Security", available at: http://www.internetgovernance.org/2011/09/20/russia-china-propose-un-general-assembly-resolution-on-information-security/

Even though Russia is a part of two cybercrime-related treaties, namely: CIS agreement on computer-related crimes[5] and Shanghai Cooperation Organisation agreement[6], provisions of these two treaties are different compare to the most recognised instruments such as aforementioned Council of Europe Convention on Cybercrime or other documents. Thus, this report is rather concentrated on providing the review and analysis of the following questions: which cyber-offences are covered by computer specific or general provisions of Russian criminal law and to which extent Russian national legislation in the area of cybercrime can be compatible with widely recognised international standards.

This report is divided into several sections in accordance with AIDP Questionnaire. Each section analyses the construction of provisions of Russian criminal legislation related to the certain types of offences. When the criminal liability for the specific offence is not provided for by Russian criminal law, the report gives this information as well.

(B) Legislative Practices and Legal Concepts

(1) How are criminal laws related to cyber-crimes codified in your country? Are they contained in a unified title or code or are they to be found in various codes or titles? (Please, provide appropriate citations).

Russian Criminal Code contains a special chapter on cybercrimes, more precisely, "computer crimes" (Chapter 28 of the Criminal Code of Russian Federation). However, this chapter covers only crimes related to confidentially, integrity and availability of computer data and systems. Other cyber-related or general provisions that apply to cybercrimes can be found in different chapters. For example, computer fraud is criminalised by the article 159.6 of the Chapter 21 (Crimes against property). As it happens in many countries, Russian criminal legislation does not contain provisions on some types of computer-related crimes, because general provisions are applicable to those offences. For example, criminal liability for "hate speech" or copyright violations is provided for by general norms without referring to the cyber-specific cases; illegal interception is covered by general provision on privacy of communications, etc.

(2) What is the impact of judicial decisions on the formulation of criminal law related to cyber-crimes?

The judicial decisions serve only for the interpretation and application of computer-specific criminal legislation. Criminal liability is provided, in accordance with the principle of legal certainty, by the provisions of criminal code only.

However, Russian Supreme court plays an important role in the application of existing provisions. One of the examples is the role of the Supreme court in the application of the provisions of Russian Criminal code to the so-called "computer fraud". Till 2012, there were no computer fraud or computer theft provisions in Russian criminal legislation. Computer fraud was punished on the basis of two articles of Russian Criminal Code: 'Swindling (Art. 159) and 'Unlawful access to the computer information' (Art. 272). This application was widely criticized in the academic literature[7]. However, the possibility of prosecuting computer fraud under the provisions of Articles 159 and 272 of

---

[5]The agreement on cooperation of the states - members of the Commonwealth of Independent States in fight against crimes in the sphere of computer information 2001.

[6] Agreement between the Governments of the Shanghai Cooperation Organization on Cooperation in the field of international security (committed in Ekaterinburg on 16 June 2009)

[7] *Tropina, Tatiana.* Kiberprestupnost: poniatie, sostoyanie, ugolovno-pravovie meri bor'bi. Vladivostok 2009; *Zykov, D.A.* Viktimologicheskie aspekty preduprezhdenija komp'juternogo moshennichestva. Avtoref. dis… kand. jurid. nauk. Nizhnij Novgorod

Russian Criminal Code was confirmed by the Juridical Decision of the Plenary Session of the Supreme Court of the Russian Federation[8] which had to be taken into account by Russian courts as the official interpretation of Criminal Code.

Nevertheless, after many years of the applications of two provisions to the cases of computer fraud, Russian Supreme court has been one of the bodies which drove the further developments of cyber-specific legislation in this field: as it has been claimed, Supreme court initiated the implementation of specific computer fraud provision into the Criminal Code of Russian Federation in 2012[9].

(3) To catch up with changing needs and circumstances and to attain new objectives, some laws are subject to frequent amendment. Normally, such amendments take the form of new laws. In certain cases these new laws, instead of simply modifying the parts of the law that need to be changed, present the required amendments into a consolidated text together with all past amendments. This technique is called recasting. Is that how cyber-crime laws are updated and adapted to changed realities in your country? Please provide appropriate references and citations.

In Russia all amendments to the cybercrime-related provisions modify the specific articles of the Criminal Code or introduce the new provisions which are incorporated in the Code. Thus, the technique which is used for changing the legislation modifies the parts of the law that need to be updated or amended. The official text of the Criminal Code does not contain the text of all past amendments if they are not in force anymore. The recasting technique, which is normally aimed to provide a comprehensive overview of all changes into specific area of regulation, is not used as an approach for amending criminal legislation. However, one can always see if the particular article has been amended, when it was amended and by which laws, because the new amended version of the Criminal Code usually contains the information about specific laws which have modified the article.

(C) The Specific Cybercrime Offenses

(1) Concerning mens rea, must cybercrime offenses be intentional? Do they require a specific intent?

(2) Are there also negligent offenses in this field?

(3) If yes, please, provide a list of those offenses.

All cybercrime offences in Russia are required to be committed intentionally. Till some years ago, however, there used to be, exceptions. For example, an offence "Violation of the rules of the operation of computers and computer

---

(2002), *Brazhnik, S.D.* Prestuplenia v sfere kompiuternoi informacii: problem kvalifikacii i zakonodatelnoi tehniki. Avtoreferat dissertacii na soiskanie uchenoi stepeni kandidata uridicheskih nauk. Izhevsk, 2002; *Hiluta, V.* "Kompiuternie" hisheniya. N 1 Zakonnost, (2009); *Tropina. Tatiana.* "Kompiuternoe moshennichestvo: voprosi kvalifikacii i zakonodatelnoi tehniki. N 6, Sviazinvest (2006); *Shirokov, V.A., Bespalova, E.V.* Nekotorie voprosi borbi s prestupnostiu v sfere telecommunikaciy i kompiuternoi informacii. N 2 Vlast i upravlenie na Vostoke Rossii (2007), P. 138.

8 Juridical Decision of the Plenary Session of Russian Criminal Court on the criminal cases of swindling, Misappropriation or Embezzlement N 51, 27th December, 2007.

9 Vishaya sudebnaya instancia razrabotala popravki v Ugolovniy Kodeks, detaliziruushie moshennichestvo. April 2012. Available at: http://www.rg.ru/2012/04/06/syd.html

networks" covered acts of the gross negligence (grave consequences) as aggravated crime. However, these articles were amended two years ago to cover *only acts committed intentionally*.

(a) Integrity and functionality of the IT system

1. Illegal access and interception of transmission

Illegal access

Criminal liability for illegal access is provided for by the Article 272 of Russian Criminal Code:

Art. 272

Unlawful access to the computer information protected by a law, that is, if this act entailed to destruction, blockage, modification, or copying of information, shall be punished…

Object. The object of the crime is "computer information" which is, according to the explanatory note to the article 272, *information (communication or data) which are represented in the electronic form, no matter which devices are used to store, process or transmit this information.* According to this definition, the object of illegal access is "data" and not system or part of the system. The object of crime has also one more characteristic: the data shall be "protected by a law". Russian Criminal Code does not define what it means, and, thus, refers to the other fields of legislation that protect specific information, like the Federal Law on Information, Information Technologies and Protection of the Information 2006[10]. This law, in turn, also does give exact definition of the 'information protected by law' rather defining the possibility to restrict access to the information and stipulating that the owner of the information establishes the rules and the restrictions regarding to the access to the information[11]. Thus, it is not completely clear what is the object of the crime provided for by Article 272 because the other parts of the legislation that do not give the exact definition.

Acts covered. There are two specific points concerning the acts covered by the Art. 272 (Unlawful access) that differ from the international standards and provide some discussions concerning their controversy: firstly, the definition of "*unlawful access*" and, secondly, the attachment of the *effect on data* to the act of illegal access.

The use of the term "*unlawful access*" has been criticized in the academic literature[12]. The word 'unlawful' in Russian can possibly have two meanings – firstly, it can mean 'in contradiction with legal rules', and, secondly, 'without right'. It creates the controversies in the interpretation of the article, for example, while some papers construe the 'unlawful access' as the 'access which is not permitted by law'[13], the others refer to the absence of authorization from the owner of the information[14].

---

10 Federal Law on Information, Information Technologies and Protection of the Information N 149-ФЗ, 27th of July, 2006

11 *Zinina, Uliana* Viktorovna. Prestuplenia v sfere kompiuternoi informacii v rossiyskom i zarubezhnom ugolovnom prave. Avtoreferat dissertacii na soiskanie uchenoi stepeni kandidata uridicheskih nauk. Moskva, 2007

12 *Bayev, M.O., Skryl, S.V.* Problemi kvalifikacii prestupleiy v otnoshenii inormacii kompiuternih system. N 1 Vestnik Voronezhskogo Instituta MVD Rossii (2007);

13 *Zinina, Uliana* Viktorovna. Prestuplenia v sfere kompiuternoi informacii v rossiyskom i zarubezhnom ugolovnom prave. Avtoreferat dissertacii na soiskanie uchenoi stepeni kandidata uridicheskih nauk. Moskva, 2007; *Brazhnik, S.D.* Prestuplenia v

The second controversy is that the Article 272 of the Russian Criminal Code does not criminalise mere illegal access to computer data. Neither can it be compatible also to the international standards that provide the possibility to criminalise illegal access committed by bypassing security measures or with dishonest intent. Instead, it requires the act of illegal access to be committed with the consequences such as modification, blockage, destruction or copying of data. *Corpus delicti* of Article 272 requires the direct casual nexus between cause (unlawful access) and effects (destruction, blockage, modification, or copying of information). However, as it is pointed out in some academic papers, the literal interpretation of the article 272 in conjunction with the principle of legal certainty means that the effect should be caused by unlawful access, e.g. access itself as a process should entail the consequences directly[15]. However, illegal access itself is the only first step to the further manipulation with information or committing other crimes. Moreover, it is also frequently indicated that the construction of the Article 272 which requires the effect that should be caused by illegal access makes it lawful to commit the acts of access aimed to the acquaintance with the protected information without its copying or without making any effects on data. Sometimes for offender it is enough only to read the information without copying to use it for illegal purposes[16]. It is also not clear how this provision can be applicable to the cases of data interference committed without accessing the data illegally.

Compare to the international standards, provided, for example, by Council of Europe Convention or Commonwealth Model Law, Russian article on illegal access merges two separate crimes: illegal access and data interference. What is considered to be an offence of data interference by the international standards (no matter if this offence is committed in conjunction with illegal access or not) in Russian legislation is attached to the act of illegal access as necessary consequences that illegal access shall have on the data in order to be a criminal offence.

Therefore, compare to the international standards, Russian Criminal Code provision stipulating legal responsibility for illegal access has limited criminalisation of both illegal access and data interference by requiring additional circumstances, namely destruction, blockage, modification, or copying of information.

Illegal interception

Illegal interception in Russian cybercrime legislation is covered by the general provision on privacy of communications (Art. 138 of the Russian criminal code which stipulates criminal responsibility for the violation of secrecy of communications).

---

sfere kompiuternoi informacii: problem kvalifikacii i zakonodatelnoi tehniki. Avtoreferat dissertacii na soiskanie uchenoi stepeni kandidata uridicheskih nauk. Izhevsk, 2002.

14 Kommentariy k Ugolovnomu Kodeksu Rossiyskoi Federacii (Editor: *Chuchaev, A.I.*), Moscow (2004). P. 625; *Volevodz, A.G.* Rossijskoe zakonodatel'stvo ob ugolovnoj otvetstvennosti za prestuplenija v sfere komp'juternoj informacii. N9 Rossijskij sud'ja. (2002).

15 *Tropina, Tatiana.* Kiberprestupnost: poniatie, sostoyanie, ugolovno-pravovie meri bor'bi. Vladivostok 2009
Brazhnik, S.D. Prestuplenia v sfere kompiuternoi informacii: problem kvalifikacii i zakonodatelnoi tehniki; Avtoreferat dissertacii na soiskanie uchenoi stepeni kandidata uridicheskih nauk. Izhevsk, 2002.

16 Bykov, V.M. and Cherkasov, V.N. Noviy zakon o prestupleniyah v sfere kompiuternoi informacci: statia 272 UK RF. In: „Rossiski sudia", 2012, Vol. 5

2. Data and system interference

As it was mentioned afore, Russian criminal legislation does not provide specific article criminalising data interference, but merges provisions on data interference with the provision on illegal access to data and attaching effect on data as necessary element of the offence of illegal access.

However, there is one provision in the Chapter 28 of Russian Criminal Code, namely Article 274 that can be (though only to some extent) compatible to the international standards of criminalising system interference.

Article 274 of Russian Criminal Code stipulates criminal responsibility for the offense that is not covered by the international standards. It criminalizes the violation of rules for operation of computer, computer systems or network thereof:

Art. 274

A violation of rules for the operation of the means of storing, processing, transferring of computer information protected by law or information-telecommunications networks and terminal equipment thereof, or rules of access to the information-telecommunication networks which entailed the destruction, blockage, modification or copying of computer information protected by a law, if this act caused material harm, shall be punished…

Object. The object of crime is in line with international standards: computer data (information protected by law) or computer system. The only concern regarding the object is the interpretation of the definition of the "information protected by law" which has been discussed afore in the analysis of the illegal access provision.

Acts covered. The construction of *corpus delicti* of the offence provided for by article 274 differs from the international approaches to criminalisation of data and system interference and raises some controversies concerning its application. Number of Russian academic papers[17] criticised this article for poor construction and vague language. First of all, it refers to the 'rules for the operation' which are not defined by any part of the Russian legislation. Given that the rules for the operations of the computers are not legally established, it is not clear which rules should be violated in order for the act to be criminal. Legislator does not clarify if it should be technical rules for the operation or the rules of the work with some kind of programs, or the rules of the work with the computer data. According to the practical interpretation of the article, these rules should be established individually in each case (by company, employer, etc.)[18]. However, this construction makes the provisions of Article 274 to be *tabula rasa*, when the borders of criminal act are not established precisely[19].

The principle of legality established by Article 3 of Russian Criminal Code stipulates that the criminality of a deed, and also its punishability and other legal consequences shall be determined only by Criminal Code. In the case of

---

17 *Lopashenko, N.A.* Ugolovno-pravovaja i kriminologicheskaja politika gosudarstva v oblasti vysokih tehnologij. Informacijni tehnologii ta bezpeka. Kiev, 2003. P. 88 – 90; *Tropina, Tatiana.* Kiberprestupnost: poniatie, sostoyanie, ugolovno-pravovie meri bor'bi. Vladivostok 2009

18 *Zinina, Uliana* Viktorovna. Prestuplenia v sfere kompiuternoi informacii v rossiyskom i zarubezhnom ugolovnom prave. Avtoreferat dissertacii na soiskanie uchenoi stepeni kandidata uridicheskih nauk. Moskva, 2007

19 *Lopashenko, N.A.* Ugolovno-pravovaja i kriminologicheskaja politika gosudarstva v oblasti vysokih tehnologij. Informacijni tehnologii ta bezpeka. Kiev, 2003. P. 88 – 90

Article 274 the borders of criminalization are flexible, *corpus delicti* is not properly determined[20], the interpretation of the meaning of the article shall be done by the law enforcement agencies that contradicts the principle of legality[21].

The construction of the article requires several elements in order to qualify act as a criminal offence: firstly, it is violation of the rules, secondly, destruction, blockage, or modification of computer information, and, thirdly, the infliction of material (substantial) harm. Thus, in order for the act to be criminal, it should cause two effects at the same time: effect on computer data and inflicting material harm, the borders of which are also not determined by the legislator[22]. It is unclear to which extent these two effects should be connected to each other and how the casual nexus should be established between the cause and these two effects. So, the *corpus delicti* is very complicated: the violation of rules which are not established by law should affect computer information, and this, in turn, should inflict material harm the borders of which are not determined. Apart from that, to qualify act as criminal it is necessary to establish also *mens rea* as the necessary element of crime[23].

The aim of the legislator was obviously to stipulate the responsibility for "data interference" and "system interference", e.g. the disruption of the functioning of computer networks in order to protect integrity and availability of computer systems. However, the construction of the article can not be compatible with the internationally recognised approaches to the criminalisation of data and system interference.

3. Data forgery

The Criminal Code of the Russian Federation has no cyber-specific provisions on data forgery (effect on data to make them look as they were authentic). Crimes on data forgery are covered by general provisions of criminal law, depending on the acts committed and the consequences of the forgery.

4. Misuse of Devices

Criminalisation of illegal devices designed for committing computer crimes in Russian criminal legislation is limited to the software: Article 273 of Russian Criminal Code stipulates criminal responsibility for creation, use and dissemination of malware and software designed for bypassing security measures:

---

20 *Lopashenko, N.A.* Ugolovno-pravovaja i kriminologicheskaja politika gosudarstva v oblasti vysokih tehnologij. Informacijni tehnologii ta bezpeka. Kiev, 2003. P. 88 – 90; *Kolosov, A.S., Kyriseva, O.K.* Kompiuternie prestuplenia: probleni teorii i praktiki. N 4 Vestnik Vladimirskogo Juridicheskogo Instituta (2008). P. 149

21 *Lopashenko, N.A.* Ugolovno-pravovaja i kriminologicheskaja politika gosudarstva v oblasti vysokih tehnologij. Informacijni tehnologii ta bezpeka. Kiev, 2003. P. 88 – 90.

22 *Tropina, Tatiana.* Kiberprestupnost: poniatie, sostoyanie, ugolovno-pravovie meri bor'bi. Vladivostok 2009; *Lopashenko, N.A.* Ugolovno-pravovaja i kriminologicheskaja politika gosudarstva v oblasti vysokih tehnologij. Informacijni tehnologii ta bezpeka. Kiev, 2003. P. 88 – 90; *Dvoreckiy, M. U.* Optimizaciya ugolovnoi otvetstvennosti za prestuplenia v sfere kompiuternoi informacii na sovremennom etape borbi s prestupnostiu. N 3 Vestnik Tambovskogo Universiteta, Seriya Gumanitarnie nauki (2008). P. 406.

23 *Lopashenko, N.A.* Ugolovno-pravovaja i kriminologicheskaja politika gosudarstva v oblasti vysokih tehnologij. Informacijni tehnologii ta bezpeka. Kiev, 2003. P. 88 – 90.
Lopashenko, N.A. Ugolovno-pravovaja i kriminologicheskaja politika gosudarstva v oblasti vysokih tehnologij. Informacijni tehnologii ta bezpeka. Kiev, 2003. P. 88 – 90.

Art. 273

Creation, dissemination and use of harmful computer programs or other computer information deliberately designed for unauthorised destruction, blockage, modification or copying of computer information or bypassing security measures, shall be punished...

International standards usually define two types of computer misuse tools, namely, (1) software, primary designed for committing computer crimes, and (2) access codes and passwords that enable access to computer systems and data. Many countries, however, and Russia is among them, restrict criminalisation to software only, thus, limiting the approach by excluding codes from the object of criminalisation.

One of the important characteristics of the objects of the computer misuse tools offence is the purpose of the devices and tools. The common requirement provided by the international standards is that the devices covered by criminalisation of computer misuse tools shall be designed *primarily* for committing crimes. Russian legislation meets this requirement by criminalising the software which is deliberately designed for making effects on computer data.

In addition, international standards require the mental element: perpetrator has to *intend to use these tools for committing crime*. This allows solving the problem of criminalisation of dual-use tools, which can be used for both legal and illegal purposed. Russian Criminal Code does not explicitly include the requirement for the specific mental element (purpose of the perpetrator to commit crime) into the construction of the article.

The acts covered are creation, dissemination and use of the illegal devices. Possession is not criminalised.

(b) Privacy

1. Violation of Secrecy of Private Data

Violation of privacy in Russian criminal legislation is covered by general provisions, protecting any kind of information related to the person's private life, including family privacy, status, habits, preferences, etc. Artticle137 of Russian Criminal Code provides for the criminal liability for violations of privacy no matter if it happens on-line or offline. It prohibits collecting and sharing private information in any way or form. The justification for the violation can be stipulated only if the data are collected and shared with the consent of the person or if they are done in accordance with the criminal procedural legislation in compliance with the safeguards provided for the use of investigative procedures.

2. Violation of professional confidentiality

Prohibition on violation of professional confidentiality, for example, concerning medical records, is stipulated by different regulation concerning various professional activities, like, medical services, etc. However, concerning all the existing regulation, the criminal liability concerning the disclosure of private data collected in the course of professional activity is covered by the aforementioned Article 137 of the Russian Criminal Code. Article 137 which protects privacy is the general provision which covers violations protected by the variety of the other laws, including Constitution of Russian Federation (which stipulates the right for privacy and its protection) and the laws related to the professional secrecy.

3. Illegal processing of personal and private data

Personal data theft does not represent such a serious problem in Russia as, for example, in USA or in Europe. The first Russian Data Protection Law, namely, Federal Law on Personal Data, was passed in July, 2006[24] after Russia in December 2005 had ratified the Council of Europe Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data of 28.1.1981. Though the main purpose of the law is to protect the individual privacy, it is asserted that on practice the Law is more about forcing compliance among negligent corporations[25].

According to the Federal Law on Personal Data, the breach of data Protection Law can be a subject of criminal liability. However, apart from 'Unlawful access to the computer information' offence (Art. 272 of Criminal Code) which is often considered as the provision which stipulates the responsibility for the breach of Law on Personal Data[26], Russian Criminal Code has only aforementioned general provision that can be applicable to the privacy offences in the area of personal data protection: Article 137 of Russian Criminal Code stipulates the responsibility for illegal collection or spreading of information about the private life of a person which constitutes his personal or family secrets, without the consent, or the distribution of this information in a public speech, in a publicly performed work, or in the mass media. This general provision can be applicable to any breach of the Law on Personal Data that infringe privacy[27]. However, there are no special provisions with regard to the privacy infringements committed in computer networks.

4. Identity theft

Russian criminal law has no specific provisions criminalising internet- or computer-related identify theft as such. Of course, different acts that constitute elements of what is called identity theft, like illegal access, acquisition of the property by using the data, etc. are covered by various provisions of Russian criminal legislation. It should be noted that there are still no international standards on the criminalisation of the internet-related identity theft; so many countries, and Russia is among them, have no specific provisions yet.

(c) Protection Against Illegal Content: ICT Related

1. Child pornography

Child pornography is criminalised in the article 242.1 of the Russian criminal Code:

---

24 Federal Law on Personal Data N 152-FZ, of 27th July, 2006.

25 See *Jellenc, E. & Zenz, K.* Global Threat Research Report: Russia. An iDefence Security Report. (2007); Russian Federation. International Intellectual Property Alliance (IIPA). 2009 Special 301 Report on Copyright Protection and Enforcement. P. 20

26 Zakon o personalnyh dannyh // available at: http://www.reignvox.ru/privacy.html; Zashita personalnyh dannyh. Zakon // available at: http://www.smbonline.ru/ru/services/personal_data.shtml; Voprosi zashiti personalnyh dannyh // available at: http://www.smbonline.ru/ru/services/personal_data.shtml

27 See: Palamarchuk, A. V. Nadzor za ispolneniem zakonodatelstva o personalnih dannih v seti Internet. In: "Zakinnost", 2010, Vol. 12

Article 242.1. Production and circulation of Materials or Articles with the Pornographic Images of Minors

Producing, procuring, storing or moving across the state border of Russian Federation for the purpose of dissemination, public showing or advertising, or dissemination, public showing or advertising, of materials or articles with pornographic images of minors, - shall be punished…

Part 2 of the Article 242.1. provides aggravated responsibility for the acts committed with the use of the Internet.

Object. Russian Criminal Code does not contain the definition of child pornography. However, there is a definition of "pornographic material" provided by the special law – Federal law 29.12.2010 N 436 on Protection of Children from the Information that Harms their Health and Development. According to this law, *information of pornographic nature is the information that is represented in the form of naturalistic images or description of the sexual organs or (and) sexual intercourse or acts of the sexual nature compatible to sexual intercourse, including the acts committed in relation to animals*. It also defines *naturalistic image or description* as *image or description of a person or (and) animal, act (or inactivity), event, phenomenon, and their consequences with focussing the attention on the details, anatomic details and physiologic processes, made in any forms and by any means*. This definition does not explicitly contains references to virtual child pornography and the so-called "look-alike" pictures, but the interpretation of the term "naturalistic images" seems to be broad enough to include *any* pornographic image of the child, be it real or virtual, or someone who looks like a child.

Acts covered. Mere possession of child abuse images is not criminalised in Russia. The article 242.1 criminalises production, procurement (which, if literally interpreted in Russian, can also include getting access to child abuse material intentionally), the acts of storing the material and moving it across the state border. Recognising the growing threat that Internet poses with regard to the child abuse, the article provides for the aggravated responsibility when all the aforementioned acts are committed by the means of the information-communication networks.

b. Any other object where criminalization depends on the use of Information & Communication Technologies (ICT)

Does your criminal law penalize the following conducts? Please cite the relevant law.

1. creation and use of true anonymity sending and/or receiving material on the ICT?

2. cyber-bullying?

3. cyber-stalking?

4. cyber-grooming?

Russian criminal legislation has no cyber-specific provisions concerning abovementioned acts.

2. Act - creation/accession/possession/transfer/public distribution by ICT (give examples)

Cite specific laws that criminalize the creation (even if never used), the accession, the possession (even if only in private), the transfer, and the public distribution through the internet and other electronic means of materials beside those already mentioned above, specifically because of internet/electronic technology use.

Apart from child abuse material, the other fields of illegal content regulation in Russia are the prohibition of extremists' activity in public communications network and information which can harm children, such as drug advertisement, suicide information, etc.

Information related to extremism and hate speech.

The responsibility for extremist-related illegal content and the possibility of closing down the web-sites containing extremists' materials are regulated on the basis of Russian Criminal Code and the so-called 'Extremism law'[28] which is considered as legislation bringing direct consequence for the Internet regulation in Russia[29].

Article 280 of Russian Criminal Codes stipulates criminal responsibility for public appeals for an extremists' activity, with the aggravating element when such a crime is committed with the use of mass media[30]. According to the Article 282 (Inciting hatred or enmity, as well as demeaning human dignity), actions carried out to incite hate or enmity as well as demean the dignity of a person or group of persons on the basis of sex, race, nationality, language, origin, relationship to religion as well as the affiliation to any social group, committed publicly or with the use of the mass media are punishable. In addition, the 'Extremism law' prohibits the use of public telecommunications network for engaging into the extremist activity[31]. One of the main goals of this law is to prevent the spread of violent content by radical groups by the obliging telecommunication operator to deactivate the content of the extremists' website as soon as it is possible; otherwise the operator has a risk to lose the license[32].

According to the 'Extremism law', extremist activity can be expressed in committing different acts, including dissemination of racists and xenophobic material, racists and xenophobic speech, terrorists' propaganda, public appeals for terrorism, nazi content dissemination and nazi propaganda. The web-site containing such materials could be taken down (or content could be removed). In addition, the list of prohibited materials (including Internet-resources) shall be made available to public.

Russian legislative provisions about extremist content can be to some extent compatible to the international standards provided by Article 3 of the Additional Protocol to the CoE Convention on Cybercrime (Dissemination of racist and xenophobic material through computer systems) that obliges each party to adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, distributing, or otherwise making available, racist and xenophobic material to the public through a computer system.

Content that can harm children

Regulation of the content that can harm children is not regulated by criminal law. However, there is a possibility to order web-site blocking, if the content is prohibited by the Federal law 29.12.2010 N 436 on Protection of Children from the Information that Harms their Health and Development.

---

28 Federal Law on Counteracting Extremist Activity No. 114-FZ of July 25, 2002.

29 *Jellenc, E. & Zenz, K.* Global Threat Research Report: Russia. An iDefence Security Report. (2007)

30 Criminal Code of the Russian Federation

31 Art. 12 of the Federal Law on Counteracting Extremist Activity No. 114-FZ of July 25, 2002.

32 See *Jellenc, E. & Zenz, K.* Global Threat Research Report: Russia. An iDefence Security Report. (2007)

(d) ICT Related Violations of Property, Including Intellectual Property

1. Fraud

As it has been mentioned afore, in 2012 Russian Criminal Code was amended to include the new provision on computer fraud:

Art. 159.6 Computer fraud

Swindling in the sphere of computer information, that is, stealing the other person's property or acquiring the right to other person's property committed by inputting, deleting, blocking, modification of computer information, or any other interference into the functioning of the systems of storage, processing and transmission of computer information or information-telecommunication networks, shall be punished....

This new article is in line with the international standards for criminalisation of computer fraud.

2. Infringement of Intellectual Property IP rights

The formation of Russian legislation in the area of intellectual property protection standards including criminal provisions stipulating the responsibility for copyright and author's rights infringements stemmed from the accession to the World International Property Organization Treaties in 1996[33]. With the new set of intellectual property laws Russia has met the international requirements for the legal protection of copyrights and author's rights[34], with the treatment of Internet content equally to the violation made by publishing books, copying CDs and DVDs in physical world[35].

Though Russian Criminal Legislation has no specific provision criminalizing infringements of copyrights and related rights with regard to the committing such a crimes by means of a computer system, two general provisions of Russian Criminal Code are applicable to the cyber-infringements in this area[36]:

- **Article 146** establishing penalties for infringement of copyright and neighbouring rights.
- **Article 147** stipulating criminal responsibility for infringement of inventors' rights and patents

According to the Article 146, the following acts are considered to be criminal offences: plagiarism that causes major harm to the rights owner; illicit use of copyrighted works or works protected by neighbouring rights; and large-scale purchase, storage and transport of counterfeit copies of works or recordings with intent to sell. A copyright infringement should be recognised as large scale if the counterfeit copies, recordings or IP use rights infringements involved have a value exceeding 100,000 Russian Roubles, and as especially large scale where the value exceeds 1 million Russian Roubles.

---

33 *Jellenc, E. & Zenz, K.* Global Threat Research Report: Russia. An iDefence Security Report. (2007)

34 *Voevodin, D.* Russia. Building and Enforcing IP Value. Salans, 2007; *Drel, M.* Recent developments in Russian trademark and copyright legislation: an update from a practising lawyer // available at: http://www.ebrd.com/pubs/legal/lit041e.pdf; *Serkov, P.* Submission from the Russian Federation. WIPO, Advisory Committee on Enforcement, 4th Session, Geneva, 1 and 2 November (2007).

35 *Jellenc, E. & Zenz, K.* Global Threat Research Report: Russia. An iDefence Security Report. (2007)

36 Cybercrime Legislation. Country Profile. Russian Federation. CoE Project on Cybercrime. Qst draft (April, 2008);

Article 147 establishes criminal responsibility for the illicit use of inventions, utility models or industrial designs; unauthorised disclosure of the substance of an invention, utility model or industrial design prior to official publication; and usurpation of inventorship or coercion into coinventorship.

Russian criminal legislation in the area of intellectual property protection does not refer to the committing the crime using the computer system. However, there are very few countries in the world which use the term 'by the means' of computer system, rather prefer to criminalize these types of infringements by using general terms 'in any manner' or 'in any other way' that actually extend the applicability of the provisions to the computer systems and cover Article infringements committed in cyberspace[37]. The concept of significant loss which is implemented in Russian legislation is in line with the requirements for the criminalisation of IP-infringements only if committed in commercial scale in order to avoid over-criminalization[38].

3. Industrial espionage

There is no computer-specific article for industrial espionage in Russia. The commercial and banking secrets are protected by the general provisions: Article 183 provides for criminal responsibility for the illegal collection of information constituting commercial secrets.

(e) Criminalization of Acts Committed in the Virtual World

Does your criminal law penalize the commission of crimes committed in the virtual world like, for example, virtual child pornography, virtual violence, virtual graffiti, cyber-defamation, sexual harassment, harassment at work, without any involvement of real persons, only virtual representation? Please cite the relevant law and provide details.

Russian criminal law has no specific provisions criminalising acts committed solely in virtual worlds.

(f) Non-Compliance Offenses

Does you criminal law penalize non cooperation with law enforcement agencies in the field of cybercrime? Duties to cooperate can be duties to retain and store information, to produce/deliver information as required by a production order, to give access to cyber systems to install filters or devices, etc. Is the breach of the duty to cooperate also enforced through administrative sanctions? Cite the relevant law and provide details.

Russian criminal legislation has no specific provisions concerning non-compliance offences in cybercrime investigations.

(D) Complementary optional information concerning law and practice (including statistics)

(1) Are cybercrimes included as such in the collection of data on crime in your country?

The official statistic of the Ministry of Interior includes the statistics on computer crime, which corresponds to the computer-specific articles of the Russian Criminal Code.

(2) Is there in your country a website that provides data and information on the occurrence, seriousness, cost, impact etc. of cyber-crimes in your country? If "yes", provide the website electronic address.

---

37 *Picotti, Lorenzo & Salvadori, Ivan*. National legislation implementing the Convention on Cybercrime: comparative analysis and good practices. Discussion paper, CoE Project on Cybercrime, August 2008. P. 34.

38 Ibid

The statistics on computer crime is a part of the big collection of the police statistics. It represents information on the occurrence of the computer crimes (showing, of course, only the number of crimes which were officially reported). The web-site is http://mvd.ru/presscenter/statistics/

(3) Do victimization surveys in your country include questions on cyber-crimes?

There are no victimization surveys on this topic.

(4) What types of computer crime / computer fraud are most often reported in your country?

It is very hard to say which crime is more frequent. First of all, the legislation is not always compatible to the international standards or the criminal liability is stipulated by the general provisions, so there is no statistics on computer-specific crimes. Secondly, there is only one source of the statistics – official data from the Ministry of Interior. It is very well known that computer crimes have high latency and high rate of underreporting. There are no victimizations surveys or organisations which carry out on-going activity of the complaint registrations from victims. For some years the threat of computer crime is widely discussed in Russia, which means that the number of crimes in IT networks is growing and cybercrimes are happening more and more frequently. However, it is very hard to say which forms of the crimes are more frequent compare to the others.

(5) Do law enforcement and prosecution in your country have a computer crimes unit? If so, how many officers/prosecutors are in it?

The police in Russia have a special department dealing with cybercrime investigation, which is called “K”-Unit. There is no publicly available information on the number of personnel working for this division.

(6) Does your or any law school in the country offer courses on cyber-crime? Please provide a website address.

To my knowledge, there are no specific legal courses on cybercrime at the Universities in Russia. Courses on criminal law at the universities usually include the analysis of the corresponding chapter of Criminal Code as a part of the education process. Many universities have, however, faculties or curses on the information security (technical side).

(7) Is the subject of cybercrime included in the training and/or continuing education of judges, prosecutors and police?

To my knowledge, there is no sustainable activity on the process of educating judges, prosecutors and the police on the specific subject of cybercrime.

(8) Please identify whether the following forms and means of cybercrime (1) occur frequently, (2) occur infrequently, or (3) have not occurred in your country, by placing an “X” as appropriate in the following table:

See the comment to the question (4) above.

Forms and Means of Cyber-	Occur frequently	Occur infrequently	Has not occurred
Online identity theft (including phishing and online trafficking in false identity information)	No data, because there is no cyber-specific provisions in the criminal law		
Hacking (illegal intrusion into computer systems; theft of information from computer systems)	x		
Malicious code (worms, viruses, malware and spyware)	x		
Illegal interception of computer data	No data, because there is only general provision in the criminal law without statistics on cyber-specific crimes		
Online commission of intellectual property crimes	No data, because there is only general provision in the criminal law without statistics on cyber-specific crimes		
Online trafficking in child pornography	x		
Intentional damage to computer systems or data	No data, because effect on computer data is attached to the crime on illegal access		