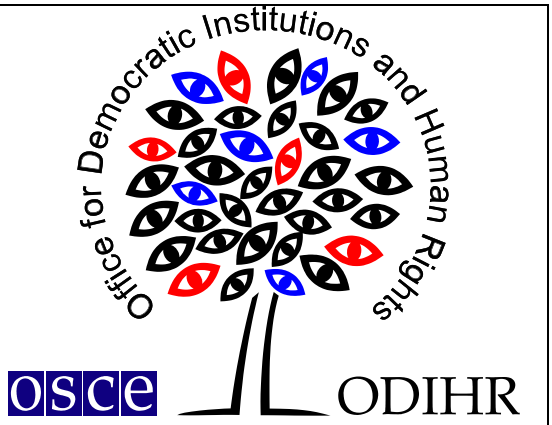
Warsaw, 22 August 2014 Opinion Nr.: CRIM-UKR/255/2014 [AlC] www.legislationline.org	

OPINION

ON THE DRAFT LAW OF UKRAINE

ON COMBATING CYBERCRIME

based on unofficial English translation of the Draft Law

This Opinion has benefited from contributions made by Professor Henrik Kaspersen, expert on cybercrime, former Chair of the Cybercrime Convention Committee (T-CY) and former Director of the Computer/Law Institute of the VU University Amsterdam.

OSCE Office for Democratic Institutions and Human Rights
Ulica Miodowa 10 PL-00-251 Warsaw ph. +48 22 520 06 00 fax. +48 22 520 0605

TABLE OF CONTENTS

Annex: Draft Law of Ukraine on Combating Cybercrime

I. INTRODUCTION

1. *By letter dated 16 June 2014, received by the OSCE Office for Democratic Institutions and Human Rights (hereinafter "OSCE/ODIHR") on 23 June 2014, the First Deputy Minister of Interior of Ukraine requested the OSCE/ODIHR to review the Draft Law on Combating Cybercrime in Ukraine (hereinafter "the Draft Law").*

2. *On 27 June 2014, the OSCE/ODIHR Director responded to this request, confirming the Office's readiness to prepare a legal opinion on the compliance of the Draft Law with international human rights standards and OSCE commitments.*

3. *This Opinion was prepared in response to the above-mentioned request.*

II. SCOPE OF REVIEW

4. The scope of this Opinion only covers the Draft Law submitted for review. Thus limited, it does not constitute a full and comprehensive review of the entire legal and institutional framework relating to combating cybercrime in Ukraine. In particular, the opinion does not address issues pertaining to the definition of cybercrime under the Criminal Code, criminal procedure rules and provisions relating to mutual legal assistance in criminal matters.

5. The Opinion raises key issues and provides indications of areas of concern. In the interest of conciseness, the Opinion focuses more on problematic areas rather than on the positive aspects of the Draft Law. The ensuing recommendations are based on relevant international standards and OSCE commitments, as well as good practices from other OSCE participating States.

6. This Opinion is based on an unofficial translation of the Draft Law, which has been attached to this document as an Annex. Errors from translation may result.

7. In view of the above, the OSCE/ODIHR would like to mention that this Opinion is without prejudice to any written or oral recommendations or comments to the Draft Law or related legislation that the OSCE/ODIHR may make in the future.

III. EXECUTIVE SUMMARY

8. At the outset, the OSCE/ODIHR welcomes Ukraine's willingness to seek international expertise on the Draft Law and the political will it has demonstrated to enhance the fight against cybercrime.

9. However, the provisions of the Draft Law may potentially lead to dangerous interference with fundamental rights and freedoms and lack substantive and procedural safeguards required according to international standards. Overall, the purpose and scope of the Draft Law should be reconsidered entirely; it should focus more on cybersecurity issues and prevention of cybercrime, and institutional frameworks for that purpose, and not so much on criminalization, criminal investigation and prosecution of cybercrimes. Particularly, given their potential to encroach on fundamental rights and freedoms, all provisions of the Draft Law pertaining to the definition of (new) criminal offences and introduction of (new) investigative measures and/or prosecution powers should

be transferred to relevant criminal and criminal procedure legislation. Moreover, it would be advisable for the drafters and relevant stakeholders to carry out a comprehensive review of the Criminal Code and Criminal Procedure Code to ensure that the definitions of cybercrime comply with the Council of Europe (hereinafter "CoE") Convention on Cybercrime[1] (hereinafter "the CoE Cybercrime Convention") and that all investigative instruments provided for in the Convention are available according to Ukrainian criminal procedure rules. In that respect, adequate substantive and procedural safeguards and guarantees in accordance with international standards should be provided in the Criminal Procedure Code. Furthermore, the drafters should re-consider imposing burdensome and costly obligations on internet service providers pertaining to data retention outside of any criminal investigation context. Finally, any measures relating to restrictions of internet access, given their impact on fundamental rights and freedoms, should be exclusively ordered by courts, and not by administrative bodies.

10. The OSCE/ODIHR thus recommends as follows:

1. Key Recommendations

A. to reconsider the overall purpose and scope of the Draft Law to focus more on cybersecurity issues and prevention of cybercrime, and the institutional framework for that purpose, rather than on criminalization, criminal investigation and prosecution of cybercrimes; [pars 18-20, 32 and 37-38]

B. to remove all provisions of the Draft Law pertaining to the definition of (new) criminal offences and introduction of (new) investigative measures and include them, as appropriate, in the Criminal Code and Criminal Procedure Code of Ukraine; [pars 17, 24-28, 43, 46-51, 63, 77-78, 83 and 86]

C. to delete from Article 5 of the Draft Law references to prosecution by executive bodies and specify that criminal prosecution of cybercrime shall be conducted exclusively by the Public Prosecutor's Office of Ukraine, in accordance with the provisions of the Criminal Procedure Code of Ukraine and other relevant legislation pertaining to prosecution; [par 41]

D. to remove references to measures of surveillance from the Draft Law and consider including them in the Criminal Procedure Code instead, provided that all substantive and procedural safeguards and guarantees stated in international standards are complied with, including those relating to personal data protection; [pars 44-48]

E. to modify the obligation of systematic data retention imposed on service providers by Article 12 par 1 (b) and (f) of the Draft Law, by specifying that such an obligation may only be applied as part of investigative measures adopted in the context of criminal investigation, and supplement the Criminal Procedure Code to provide for the possibility to resort to such investigative measures, including via fast-track procedures; [pars 59-65]

[1] The CoE Convention on Cybercrime (CETS No. 185) was signed by Ukraine on 23 November 2001, ratified on 10 March 2006 and entered into force in Ukraine on 1 July 2006.

F. to delete from Article 13 of the Draft Law references to the grounds justifying limitations to the use and access to the Internet/ICTs which are not in line with international standards and consider replacing them with 'legitimate' grounds according to international standards, while ensuring that only a court, and not an administrative body, will be competent to order such limitations, as necessary, based on a petition of the Prosecutor General in accordance with the Criminal Procedure Code; [pars 67-78]

G. to carry out an in-depth review of the Criminal Code and Criminal Procedure Code to ensure that all criminal offences and investigative instruments contemplated in the CoE Cybercrime Convention are included therein, and as appropriate, supplement the provisions relating to general criminal offences to specify that they cover acts committed through the use of ICTs, including the Internet; [pars 25-28 and 49]

2. Additional Recommendations

H. to ensure the coherence of the provisions of the Draft Law with the Criminal Code and the Criminal Procedure Code, and make cross-references to the provision of the Criminal and Criminal Procedure Codes whenever relevant; [pars 17, 24 and 41]

I. to consider simplifying and merging the definitions provided in Article 1 and in Article 3 of the Draft Law and only include the definitions that are necessary for the understanding of the later provisions of the Draft Law, covering also the definition of "cybersecurity"; [pars 22 and 31-32]

J. to supplement Article 4 to provide that the New Cybercrime Body is tasked with raising awareness and providing expertise on cybersecurity issues, including ICT security, to the government, law enforcement, enterprises, academia and the public in general; [pars 37-38]

K. to consider supplementing the Criminal Procedure Code with provisions relating to digital forensics, as well as electronic evidence and their lawful use before court; [pars 50-51]

L. to delete Article 6 or 9 of the Draft Law since they are identical in content and ensure that the co-operation between state authorities and non-government actors occurs on a voluntary basis and exclude the reference to the "[re]solution of crimes and discovery of perpetrators" which should be addressed under the Criminal Procedure Code; [pars 53-55]

M. to delete Article 10 of the Draft Law; [par 55]

N. to amend Article 13 of the Draft Law so that the National Commission for Protection of Information and Information Technologies may no longer order communication operators to suspend internet access and hosting providers to delete allegedly illegal data; instead, the National Commission should have more general oversight and monitoring powers; [par 77]

O. to consider amending and supplementing Article 19 of the Draft Law relating to international co-operation as follows:

1) include the possibility for spontaneous information of other States when the safeguards mentioned in the CoE Cybercrime Convention are provided; [par 82]

2) provide the possibility for Ukrainian authorities to request another State to order or obtain the expedited preservation of data; [par 83]

3) specify that "dual criminality shall not be required as a condition to providing such preservation"; [par 84]

4) include a list of specific instances when a request for data preservation may be refused, in accordance with Article 29 of the CoE Cybercrime Convention; [par 85]

P. to supplement the Criminal Procedure Code to ensure that the expedited preservation of data, as well as the renewal of the preservation order, is possible, and ensure that all the conditions and safeguards provided by Articles 16 and 29 of the CoE Cybercrime Convention are included; [par 86]

Q. for the drafters and stakeholders:

1) to discuss in more detail the scope and modalities for data collection as well as structure and management of the database relating to cybercrimes and amend the Draft Law as appropriate; [par 39] and

2) to consider the possibility to establish a new body that would specialise in digital forensics and handling of electronic evidence. [pars 50-51]

IV. ANALYSIS AND RECOMMENDATIONS

1. International Standards

11. This Opinion analyzes the Draft Law from the viewpoint of its compatibility with international standards and OSCE commitments. The main international instrument pertaining to the prevention of and fight against cybercrime is the CoE Cybercrime Convention, together with its Additional Protocol concerning the criminalization of acts of a racist and xenophobic nature committed through computer systems.[2]

12. Key general international human rights instruments applicable in Ukraine include the European Convention on Human Rights and Fundamental Freedoms (hereinafter "the ECHR")[3] and the International Covenant on Civil and Political Rights (hereinafter "the ICCPR").[4] Both instruments protect key human rights and fundamental freedoms such as, *inter alia*, the right to freedom of peaceful assembly, freedom of expression, the right to respect for private and family life and the right to a fair trial.

[2] The Additional Protocol to the CoE Cybercrime Convention concerning the criminalization of acts of a racist and xenophobic nature committed through computer system (CETS No. 189) was signed by Ukraine on 8 April 2005, ratified on 21 December 2006 and entered into force in Ukraine on 1 April 2007.

[3] The European Convention on Human Rights and Fundamental Freedoms was ratified by Ukraine and entered into force on 11 September 1997.

[4] The UN International Covenant on Civil and Political Rights, was adopted by General Assembly resolution 2200A (XXI) on 16 December 1966 and ratified by Ukraine on 12 November 1973.

13. The domestic legal framework pertaining to the prevention of and fight against cybercrime should not encroach upon these international human rights. Content available on the Internet is, in principle, subject to the same human rights regime as traditional media, such as printed matter and speech. Resolution 20/8 of the United Nations Human Rights Council affirms that the "same rights that people have offline must also be protected online, in particular freedom of expression, which is applicable regardless of frontiers and through any media of one's choice".[5]

14. In addition, various OSCE commitments on preventing and combating terrorism[6] also touch on the use of the Internet for terrorist purposes.[7] Other commitments focus on the criminal use of information and communication technologies and illegal activities endangering cybersecurity.[8] In particular, OSCE participating States committed to become party to and to implement the obligations under the CoE Cybercrime Convention, amongst others.[9] In that respect, the OSCE/ODIHR offers, upon request by participating States, technical expertise on the implementation of international anti-terrorism conventions and protocols as well as on the compliance of legislation with international standards.[10]

15. It must be further highlighted that when dealing with online content that is illegal under their national legislation and is hosted within their jurisdiction, OSCE participating States have committed "to take all appropriate action against such content and to co-operate with other interested States, in accordance with their national legislation and the rule of law, and in line with their international obligations, including international human rights law".[11]

2. General Comments

16. At the outset, it is noted that the Draft Law contains provisions addressing a variety of matters, ranging from the definition of crimes, measures relating to their investigation and prosecution, their prevention, the establishment of a new body in charge of certain cybercrime-related issues, as well as measures more generally addressing Information Communications Technology (hereinafter "ICT") security.

17. First of all, it is unclear why the Draft Law defines certain criminal acts at all, without including at least cross-references to relevant provisions of the Criminal

---

[5] See par 1 of the 2012 Resolution 20/8 of the UN Human Rights Council on the Promotion, Protection and Enjoyment of Human Rights on the Internet, A/HRC/RES/20/8, 16 July 2012, available at http://ap.ohchr.org/documents/dpage_e.aspx?si=A/HRC/RES/20/8.

[6] Annex to Ministerial Council Decision No. 1 on Combating Terrorism: The Bucharest Plan of Action for Combating Terrorism, MC(9)DEC/1, 4 December 2001; and the OSCE Charter on Preventing and Combating Terrorism, MC(10).JOUR/2, 7 December 2002.

[7] The "use of the Internet for terrorist purposes" has been interpreted comprehensively as the use of the Internet by terrorist organizations "to identify and to recruit potential members, to collect and transfer funds, to organize terrorist acts, to incite terrorist acts in particular through the use of propaganda" (see e.g. Sofia Ministerial Council Decision on Combating the Use of the Internet for Terrorist Purposes, MC.DEC/3/04, December 2004).

[8] See par 6 of Decision No. 1106 Initial Set of OSCE Confidence-Building Measures to reduce the Risks of Conflict Stemming from the Use of Information and Communication Technologies, PC.DEC/1106, 3 December 2013.

[9] See par 3 of Decision of the Ministerial Council No. 7/06 on Countering the Use of the Internet for Terrorist Purposes, MC.DEC/7/06, 5 December 2006.

[10] *Op. cit.*, footnote 6, par 18 (OSCE Bucharest Plan of Action for Combating Terrorism)

[11] See *op. cit.*, footnote 9, par 5 (2006 Decision on Countering the Use of the Internet for Terrorist Purposes).

Code, given that Article 3 of the Criminal Code of Ukraine expressly provides that "[t]he criminality of any act as well as its punishability and other criminal consequences shall be determined exclusively by this Code". Similarly, according to Article 3 of the Criminal Procedure Code, "[c]riminal proceedings are conducted in the territory of Ukraine in accordance with the present Code wherever a crime has been committed". Thus, investigative measures and prosecution should in principle be exclusively regulated by the Criminal Procedure Code. This is also important to ensure that powers to control, prevent and investigate crimes are exercised in a manner which fully respects due process and other guarantees which legitimately place restraints on criminal investigations and prosecution.[12] It is therefore recommended that all provisions of the Draft Law pertaining to the definition of (new) criminal offences and introduction of (new) investigative measures and/or prosecution powers be removed from the Draft Law and included, as appropriate in the Criminal Code and Criminal Procedure Code (see more comments on these aspects in pars 24-27, 37, 43, 47-51, 63, 78, 82 and 85 *infra*). To avoid any ambiguity, the Draft Law could explicitly state that the investigation and prosecution of cybercrimes are carried out in accordance with the provisions of the Criminal Procedure Code.

18. From a more strategic point of view, the Draft Law does not seem to make a clear distinction between the tasks relating to the investigation and prosecution of cybercrimes and certain other measures and efforts pertaining to the broader field of so-called cybersecurity,[13] including ICT security. While greater cybersecurity can help to reduce the risk of cybercrime, the two areas should be kept separate since the competences of the entities in charge of these respective areas are very different in nature and in scope. Both types of entities may need to share and exchange information and expertise, but only where necessary for the fulfilment of their individual tasks, and by virtue of precise legal procedures.

19. At the same time, it must be highlighted that the scope of the Draft Law is too narrow to address all issues pertaining to cybersecurity in its broadest sense. It may be helpful for the drafters and stakeholders to discuss the objectives, purpose and scope of the Draft Law in greater detail. When doing so, they may consider broadening the scope of the Draft Law to cover in a more comprehensive manner all aspects relating to cybersecurity, including the security and integrity of ICT networks, and prevention of cybercrime. In that respect, addressing the multi-dimensional challenges of fighting cybercrime would require a comprehensive approach that should also involve, next to legislation, general policies, education and awareness-raising, capacity

[12] See e.g., par 48 of *K.U. v. Finland*, European Court of Human Rights (hereinafter "the ECtHR") judgment of 2 December 2008 (Application No 2872/02), available at http://hudoc.echr.coe.int/sites/eng/pages/search.aspx#{"appno":["2872/02"],"itemid":["001-89964"]}.

[13] See the definition of "cybersecurity" contained in 2010 Resolution 181 of the UN International Telecommunication Union (hereinafter "ITU"), available at http://www.itu.int/net/itunews/issues/2010/09/20.aspx, which states that "Cybersecurity is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets. Organization and user's assets include connected computing devices, personnel, infrastructure, applications, services, telecommunications systems, and the totality of transmitted and/or stored information in the cyber environment. Cybersecurity strives to ensure the attainment and maintenance of the security properties of the organization and user's assets against relevant security risks in the cyber environment. The general security objectives comprise the following: Availability; Integrity, which may include authenticity and non-repudiation; Confidentiality".

development, research as well as technical approaches to help combat cybercrimes (e.g., antivirus software, firewalls, intrusion detection systems, etc.).[14]

20. In light of the above, the overall purpose and scope of the Draft Law should be reconsidered entirely, focusing more on cybersecurity issues and prevention of cybercrime, and establishing an institutional framework for that purpose, rather than on criminalization, criminal investigation and prosecution of cybercrimes.

21. In any case, the development of the Draft Law should have been preceded by the development of a policy to identify relevant measures and instruments to address cybercrime issues. It has been noted that countries that have merely introduced cybercrime legislation without having developed an anti-cybercrime strategy first, including policies at the government level, usually face severe difficulties, often caused by overlaps and potentially contradictory measures.[15] Further, while some of the Articles of the Draft Law seem to mirror certain provisions of the CoE Cybercrime Convention, a proper and comprehensive assessment of all the measures to be adopted in order to be in full compliance with the CoE Cybercrime Convention does not appear to have been carried out.

3. Main Definitions

22. Articles 1 and 3 of the Draft Law provide a definition of cybercrime. Article 1 refers to two terms, namely "cybercrime" which is defined as "criminal activity, connected with the use of computers, information technologies, global networks and cyberspace" and "cyber-crime" defined as "a guilty socially dangerous penal act committed by using computer technologies […]". Unless this is a result of faulty translation and unless the distinction is clear in the Ukrainian version, the use of the terminology and the respective definitions of "cybercrime" and "cyber-crime" may be confusing and somewhat redundant. If the purpose of the latter definition ("cyber-crime") is merely to provide a more detailed definition of "cybercrime", then the two should be merged. Article 3 of the Draft Law further specifies that "cybercrime" includes a number of "crimes connected with the use of computer technologies" such as cyber stalking, cyber theft, hacking, hacktivism etc. This could perhaps also be incorporated into a merged article and not necessarily be that detailed, e.g. by generally stating that for the purpose of the Draft Law, the definition of "cybercrime" should encompass the criminal offences defined by the Criminal Code committed through the use of ICTs.

23. Moreover, while the aim of defining cybercrime in a precise manner is commendable to ensure legal certainty and foreseeability, a number of general points should be raised with respect to these provisions.

24. First of all, as mentioned in par 17 *supra*, it is unclear why a separate law defines certain criminal offences in detail, without adding cross-references to the respective provisions of the Criminal Code of Ukraine. Moreover, it appears that some of these so-called "crimes" included in the Draft Law do not have their equivalent in the Criminal Code (e.g., hacking, hacktivism, stalking). Also,

[14] See page 99 of the UN ITU 2012 Report on "Understanding Cybercrime: Phenomena, Challenge and Legal Response", available at http://www.itu.int/ITU-D/cyb/cybersecurity/docs/Cybercrime%20legislation%20EV6.pdf.

[15] ibid, page 98 (2012 ITU Report on Understanding Cybercrime).

some criminal acts defined in the Draft Law partially overlap with criminal offences already provided in the Criminal Code; however, their respective definitions differ to a certain extent.[16] Such differences in terminology create potential for conflict. The predictability of law should allow potential perpetrators to foresee which legal regime will be applied to their case. It is, therefore, advised to review the legal framework on cybercrimes and to make sure that all the "crimes" referred to in the Draft Law have their equivalent in the Criminal Code. Additionally, to avoid ambiguity or conflict, the Draft Law could make cross-references to the respective definitions contained in the Criminal Code.

25. Second, Articles 1 and 3 of the Draft Law do not seem to encompass the broad range of criminal offences covered by the CoE Cybercrime Convention and its Protocol (e.g., illegal access to a computer system, illegal interception of computer data, all child pornography-related acts, acts of a racist and xenophobic nature committed through computer systems), even if some of these offences are or may be partially addressed through certain provisions of the Criminal Code.

26. At the same time, a partial review of the provisions of the Criminal Code suggests that they do not encompass the whole range of criminal offences envisaged by Section 1 of Chapter II of the CoE Cybercrime Convention[17] and its Additional Protocol on the criminalization of acts of a racist and xenophobic nature committed through a computer system (e.g., illegal access to a computer system, procuring or possession child pornography, acts of a racist and xenophobic nature committed through computer systems). This should be remedied since criminalization gaps in any country can create havens for offenders, which has the potential to affect other countries globally. Moreover, criminalization '*differences'* introduce challenges for effective international co-operation in criminal matters involving cybercrime, in particular as regards the principle of dual criminality.[18]

27. Therefore, it is recommended to the drafters to review the provisions of the

---

[16] E.g., Article 361 of the Criminal Code on the "Unauthorized interference with the work of electronic computing machines (computers), automated systems, computer networks or telecommunication networks"; Article 361-1 of the Criminal Code on the "Creation for the purpose of use, dissemination and distribution of harmful software or hardware, as well as their dissemination and distribution"; Article 361-2 of the Criminal Code on the "Unauthorized dissemination and distribution of information with restricted access, which is stored in the electronic computing machines (computers), automated systems, computer networks or information-carrying medium"; Article 362 of the Criminal Code on the "Unauthorized actions with information, which is processed in the electronic computing machines (computers), automated systems, computer networks or saved on the information-carrying medium, committed by a person entitled to access to such information"; Article 363 of the Criminal Code on the "Violation of operating rules of electronic computing machines (computers), automated systems, computer networks or telecommunications networks and the order or rules protection of information which is processed there-through"; Article 363-1 of the Criminal Code on "Impeding the work of electronic computing machines (computers), automated systems, computer networks or telecommunication networks by mass distribution of electronic messages"; Article 163 of the Criminal Code on the "Violation of privacy of mail, telephone conversations, telegraph and other correspondence conveyed by means of communication or via computers"; Article 176 of the Criminal Code on the "Violation of copyright and allied rights"; Article 190 of the Criminal Code on "Fraud".

[17] Offences covered in Articles 2-11 of the CoE Convention, including *inter alia* illegal access, illegal interception, data interference, system interference, misuse of devices, computer-related forgery, computer-related fraud, offences related to child pornography and offences related to copyrights and neighbouring rights.

[18] See page 77 of the 2013 UNODC Comprehensive Stury on Cycercrime, available at http://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf.

Criminal Code to analyse whether they are fully in line with the CoE Cybercrime Convention. The lawmakers and stakeholders should also discuss whether to go beyond the scope of the CoE Cybercrime Convention and perhaps also address other types of cyber-criminal conducts, as done in other countries (e.g., "illegal remaining in a computer system", spamming, identity theft).[19] Moreover, Article 23 of the CoE Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse requires the criminalization of the solicitation, using ICTs, of children for sexual purposes where the proposal has been followed by material acts leading to an actual meeting.[20] The Criminal Code does not seem to include such a criminal offence and should therefore be supplemented accordingly.

28. Third, it is worthwhile to highlight that certain cyber-criminal conduct (e.g., cyberfraud, cyberstalking, corporate espionage or cybertheft) may potentially be subsumed under general criminal provisions and would not necessarily need a specific definition/provision. Regarding substantive anti-cybercrime legislation, the practice varies greatly from country to country between the introduction of cyber-specific criminal provisions and/or the use of general criminal offences for criminalizing the acts falling under the scope of the CoE Cybercrime Convention.[21] However, the fact that provisions exist in the Criminal Code that are applicable to similar acts committed outside the cyber sphere does not mean that they can and will be applied to acts committed over the Internet as well.[22] Consequently, the lawmakers should carry out a thorough analysis of the current legal framework to identify any possible gaps. They should also consult with representatives from law-enforcement and criminal justice system to inquire whether the relevant general criminal provisions have been used/applied in practice for the prosecution and conviction of cybercrimes. If this is not the case, the respective provisions of the Criminal Code should be supplemented to expressly state that acts committed through the use of ICTs, including the Internet, fall under the scope of the respective general provision.

29. Fourth, certain definitions of criminal acts falling under Article 3 of the Draft Law (e.g. crimes connected with the use of computer technologies which encroach on "public morals" or "public safety", hacking defined as "the use of internet-technologies in order to hack computer network and their users" or the catch-all terminology "other cybercrimes") are relatively vague. As such, they do not respect the principle of legality (*nullum crimen, nulla poena sine lege*) i.e., that an act can be punished only if, at the time of its commission, the act was the object of a valid, sufficiently precise, written criminal law to which a sufficiently certain sanction was attached. Similarly, additional provisions of the Draft Law under Chapter III refer to "other violations of the law connected to cybercrime" such as "appeals to mass riots", "conduct of extremist activities", "participation in mass (public) activities conducted in violations of the established order" and "use of networks and/or communications means with criminal goals, which harm the interests of a person, the society and the state", which are likewise very vaguely crafted and for which no definition is provided.

---

19 *Op. cit*., footnote 14, pages 181, 206 and 213 (2012 ITU Report on Understanding Cybercrime).

20 The Article 23 of the CoE Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse (CETS No. 201) ratified by Ukraine on 27 August 2012 and in force in Ukraine since 1 December 2012, available at http://www.coe.int/t/dghl/standardsetting/children/Text_Convention_en.asp.

21 *Op. cit.*, footnote 18, page 79 (2013 UNODC Comprehensive Stury on Cycercrime).

22 *Op. cit.*, footnote 14, page 104 (2012 ITU Report on Understanding Cybercrime).

These definitions are thus also not compliant with the principles of legal certainty and foreseeability (see also par 68 *infra*).

30. Article 1 of the Draft Law contains numerous definitions, including certain general criminal offences committed using ICTs, certain cyber-specific offences as well as a number of technical definitions, pertaining to the technological aspects of cybercrime. It is noted positively that the technical definitions are overall compliant with the provisions of CoE Cybercrime Convention. For the sake of clarity though, it would be advisable to separate the technical definitions from the more substantive provisions relating to the definitions of cybercrime.

31. More generally, if criminalization and investigation/prosecution are excluded from the scope of the Draft Law as recommended in par 17 *supra*, then it may not be necessary to state in detail all these definitions and a more general definition of cybercrime would appear to be sufficient. In this context, it was also noted that many of the terms that are defined under Article 1 of the Draft Law are not even used later on in the Draft Law, which demonstrates that the related definitions may not be necessary. Moreover, the risk of stipulating such a detailed list of offences falling under the definition of "cybercrime", even if it is open-ended, entails a possibility of considering certain behaviours as falling outside of the scope of the Draft Law, if they are not expressly mentioned in Articles 1 and 3 of the Draft Law. Consequently, the drafters should review the list of definitions and only include those that are necessary for the understanding of the later provisions of the Draft Law.

32. Moreover, in light of the comment in pars 18-20 *supra* on cybersecurity, it may be useful to include under Article 1 of the Draft Law a definition of "cybersecurity", including ICT security.

4. Institutional Framework for Preventing and Combating Cybercrime

4.1. Government Bodies involved in Preventing and Combating Cybercrimes

33. Chapter II of the Draft Law pertains to the institutional framework for preventing and combating cybercrime. Article 4 of the Draft Law refers to various bodies involved directly and indirectly in preventing and combating cybercrime. It is noted that this provision does not mention the role of the prosecution services in that respect. Moreover, the allocation of respective roles and responsibilities is formulated in relatively vague terms.

34. Article 4 of the Draft Law provides for the establishment of a new permanent central body ("separate structural department") under the Ministry of Internal Affairs or, alternatively, of a new state body, the National Center for Combating Cybercrime (subordinated and reporting to the Ministry of Internal Affairs) (either entity is referred hereinafter as "New Cybercrime Body"). The OSCE/ODIHR is not in a position to comment on which of these options would be the optimal choice for Ukraine. This is more an internal organizational matter and the proper functioning of such structure will also depend on an adequate allocation of human and financial resources. However, the second option will certainly imply a greater degree of autonomy from the Ministry of Internal Affairs, though with potentially additional costs.

35. The provision stipulates that the New Cybercrime Body (whichever form it will

take) is responsible for the co-ordination of "the activities of the subjects involved in combating cybercrime" and of "the use of new technologies in countering cyber-attacks". In this context, it should be pointed out that the term "cyber-attack" is not defined in any of the other provisions of the Draft Law.

36. It is welcome that Article 4 of the Draft Law refers to the operational co-ordination with other bodies engaged in the field of cybercrime, as one of the main tasks of the new body. This is particularly important given the key role of co-operation and partnerships across ministries and between authorities, as well as private sectors, NGOs and individuals, for effective crime prevention.[23]

37. In light of the comments made in pars 18-20 *supra*, it would be advisable to consider prescribing, as the primary task of the New Cybercrime Body, the ability to raise awareness and provide expertise on cybersecurity issues, including ICT security, to the government, law enforcement, enterprises, academia and the public in general. Such functions would be preventive in nature, and could help minimize the financial and technical damages resulting from cybercrimes. These tasks should be clearly distinguished from activities of law enforcement entities and prosecution services which should be in charge of investigative measures and prosecution in accordance with the provisions of the Criminal Procedure Code. It would be helpful if the Draft Law could reflect a clearer separation of these respective tasks.

38. In many countries, the tasks related to ensuring cybersecurity, including ICT security, are handled by the so-called computer emergency (or incident) response teams (CERTs/CIRTs) which play a key role in identifying and mitigating computer system vulnerabilities and in responding to security incidents.[24] It would be advisable for the drafters to review examples from other countries[25] and international good practices[26] and supplement the Draft Law to ensure that the New Cybercrime Body has a mandate in line with such practices. The establishment of a body similar to a CERT/CIRT in Ukraine could be useful, particularly as regards the co-ordination and exchange of information, including at the international level, with other entities engaged in cybersecurity policies and measures.

39. Finally, Article 5 of the Draft Law provides that the New Cybercrime Body "prepares and recurrently updates databases on criminal activities involving computer technologies". It must be noted in that respect that the various bodies listed under Articles 4 and 5 of the Draft Law may have different needs in terms of data collection. For instance, the Security Services and the Ministry of Defence will need intelligence related to their respective fields of investigation while the Ministry of Internal Affairs would need criminal justice statistics and

---

[23] See par 9 of the UN Guidelines for the Prevention of Crime, UNECOSOC Resolution 2002/13, 24 July 2002, available at https://www.unodc.org/documents/justice-and-prison-reform/crimeprevention/resolution_2002-13.pdf.

[24] *Op. cit.*, footnote 18, page 230 (2013 UNODC Comprehensive Stury on Cycercrime). See also Resolution 58 of the World Telecommunications Standardization Assembly (2012) encouraging the creation of national computer incident response teams, particularly for developing countries, available at http://www.itu.int/en/ITU-T/wtsa12/Documents/resolutions/Resolution%2058.pdf.

[25] For example, in 2003, the US Department of Homeland Security created US-CERT. The Department of Homeland Security's United States Computer Emergency Readiness Team (US-CERT) leads efforts to improve cybersecurity posture, co-ordinate cyber information sharing, and manage cyber risks.

[26] See e.g., the European Union Agency for Network and Information Security, "A Setp-by-step Approach to set up a CSIRT" (2006), available at http://www.enisa.europa.eu/activities/cert/support/guide.

the New Cybercrime Body, information about security incidents. The drafters and stakeholders should discuss in more detail the information needs of the different bodies and the types of data to be collected, which will determine the scope and modalities for data collection and structure and management of the database.

4.2. Criminal Prosecution

40. More specifically, Article 5 of the Draft Law pertains to the authority of competent state bodies and institutions in charge of preventing and combating crimes in the field of computer information. The provision vests the Ministry of Internal Affairs and the Security Service, as well as their respective structural departments, with the competence to, *inter alia*, carry out criminal prosecution.

41. Unless a result of faulty translation, it would appear that this provision provides for the ability for executive bodies to initiate and conduct criminal prosecution. The procuracy, as an entity separate from the executive, legislative and judicial branches in Ukraine,[27] appears to be the unique authority with the responsibility to prosecute alleged criminal offences. Moreover, every decision of a public prosecutor which interferes with the fundamental rights and freedoms of any other person should be subject to judicial control.[28] Such prerogatives should not be part of the competence of the executive, all the more given the importance of securing the independence or autonomy of prosecution services.[29] It is strongly recommended to revise Article 5 of the Draft Law to delete the reference to criminal prosecution as it relates to executive bodies and specify that criminal prosecution of cybercrime is the exclusive competence of the Public Prosecutor's Office of Ukraine and is carried out in accordance with the provisions of the Criminal Procedure Code of Ukraine and the relevant legislation pertaining to prosecution services.

4.3. Criminal Investigative Measures, including Surveillance Measures

42. Article 7 of the Draft Law stipulates that the Ministry of Internal Affairs provides equipment necessary for combating cybercrime. The provision fails to specify, however, in which way and in which instances, law enforcement officials could lawfully use such equipment for the purpose of criminal investigations. More specifically, Article 7 of the Draft Law seems to imply the possibility of resorting to covert measures of surveillance.

43. First of all, as regards criminal investigation measures, as mentioned par 17 *supra*, these should not be included in the Draft Law but rather in the Criminal Procedure Code as per Article 3 of the Criminal Procedure Code, all the more given their potential impact on human rights and fundamental freedoms.

---

[27] See pages 2 and 3 of the replies from Ukraine to the Questionnaire of the Consultative Council of European Prosecutors, 7 February 2012, available at http://www.coe.int/t/dghl/cooperation/ccpe/opinions/travaux/OP_7_Ukraine.pdf.

[28] See par 31 of Recommendation Rec(2000)19 of the CoE Committee of Ministers to member states on the role of public prosecution in the criminal justice system, adopted on 6 October 2000, available at https://wcd.coe.int/ViewDoc.jsp?id=376859&Site=CM. See also the Joint Opinion of the European Commission for Democracy through Law (Venice Commission) and the Directorate for Human Rights of the CoE on the Draft Law on the Public Prosecutor's Office of Ukraine, CDL-AD(2013)025, 14 October 2013, available at http://www.venice.coe.int/webforms/documents/default.aspx?pdffile=CDL-AD(2013)025-e.

[29] See par 30 of the Venice Commission Report on the Independence of the Judicial System – Part II: The Prosecution Service (2010), available at http://www.coe.int/t/dghl/cooperation/capacitybuilding/Source/judic_reform/europeanStandards_en.pdf.

44. It is important to stress that the right to privacy as prescribed by Article 8 of the ECHR guarantees the right to respect for private and family life, home and correspondence. The acquisition and recording by the state of information on individuals obtained through surveillance, interception of communication or undercover operations must, therefore, be provided by law, and must be justified, necessary, proportionate and non-discriminatory. It should especially be borne in mind that according to Article 15 of the CoE Cybercrime Convention, "the establishment, implementation and application of the powers and procedures […] are subject to conditions and safeguards provided for under its domestic law, which shall provide for the adequate protection of human rights and liberties, including rights arising pursuant to obligations it has undertaken under the [ECHR], the [ICCPR], and other applicable international human rights instruments, and which shall incorporate the principle of proportionality". Consequently, specific criminal investigations or proceedings should be subject to certain conditions and safeguards, *inter alia* judicial or other independent supervision, clear grounds justifying application and limitation of the scope and duration of the power or procedure, as per Article 15 par 2 of the CoE Cybercrime Convention.

45. In the context of secret measures of surveillance by public authorities, because of the lack of public scrutiny and the risk of misuse of power, compatibility with the rule of law requires that domestic law provides adequate protection against arbitrary interference with Article 8 of the ECHR rights, i.e., the existence of adequate and effective guarantees against abuse.[30]

46. Any legislation pertaining to measures of surveillance should therefore comply with the minimum safeguards provided for in the case-law of the European Court of Human Rights' (hereinafter "the ECtHR"). First, the legislation should be clear and accessible.[31] An individual should be able to foresee the conditions and circumstances in which the authorities are empowered to resort to the "special investigative activities". The legislation should provide clear grounds for ordering the measures of surveillance. In particular, it should specify the nature of offences which may give rise to an interception order and provide a definition of the categories of people liable to have their communications monitored, and in which circumstances; define the scope and state a limit on the duration of such monitoring; identify the authorities competent to permit, carry out and supervise the surveillance measures; specify the procedure to be followed for examining, using and storing the data obtained; include the precautions to be taken when communicating the data to other parties; and detail the circumstances in which data obtained may or must be erased or the records destroyed.[32] In addition, there should also be some form of oversight of the surveillance measures undertaken by an external body or official, or public reporting mechanism of some type, which should be independent.[33] The Draft

---

30 See par 63 of *Uzun v. Germany*, ECtHR judgment of 2 September 2010 (Application No 35623/05), available at http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-100293#{"itemid":["001-100293"]}.

31 See e.g., par 27 of *Kruslin v. France*, ECtHR judgment of 24 April 1990 (Application No 11801/85), available at http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-57626#{"itemid":["001-57626"]}.

32 See par 76 of *Association for Eurtopean Integration and Human Rights and Ekimdzhiev v. Bulgaria*, ECtHR judgment of 28 June 2007 (Application No 62540/00), available at http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-81323#{"itemid":["001-81323"]}. See also *op. cit.*, footnote 30, par 63 (*Uzun v. Germany*, ECtHR judgment of 2 September 2010).

33 ibid. pars 85 and 87-88 (*Association for Eurtopean Integration and Human Rights and Ekimdzhiev v. Bulgaria*, ECtHR judgment of 28 June 2007).

Law currently does not fulfil these requirements and this may potentially lead to dangerous interference with the right to respect for private life and correspondence.[34] It must be pointed out that Article 14-1 of the Criminal Procedure Code seems to provide for the possibility to carry out certain surveillance measures of telephone and other conversations but does not seem to list the above-mentioned substantive and procedural safeguards. It is further not clear whether the provision applies to electronic communications. Therefore, it would be advisable to revise this Article.

47. Moreover, adequate and effective guarantees against the risk of misuse or abuse of power by public authorities, including adequate remedies in case of abuse, must be in place.[35] This is particularly important where the State stores personal information in the interests of national security.[36] Furthermore, the compiling, storing, use and disclosure of personal information by the State should comply with the provisions of the CoE Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data.[37] There should also be some rules specifying with an appropriate degree of precision, the manner of screening of the intelligence obtained through surveillance and/or the procedures for preserving its integrity and confidentiality and for its destruction.[38] Finally, the legislation should also provide for a mechanism whereby the individual subject to surveillance should be informed as soon as notification can be made without jeopardizing the purpose of the surveillance after its termination[39]. Neither the Draft Law nor the Criminal Procedure Code seems to provide such guarantees and safeguards.

48. In light of the above, all references to these 'new' investigative measures, in particular the "covert measures of surveillance" referred to in Article 7 of the Draft Law, should be removed from the Draft Law. The drafters should discuss the possibility to amend the Criminal Procedure Code to include such measures, provided that all the substantive and procedural safeguards and guarantees described in pars 44-47 *supra*, are provided.

49. More generally, the drafters should review the provisions of the Criminal Procedure Code and supplement them as appropriate to ensure that the

---

[34] ibid. pars 71 and 75 (*Association for Eurtopean Integration and Human Rights and Ekimdzhiev v. Bulgaria,* ECtHR judgment of 28 June 2007). See also CoE Committee of Ministers, Recommendation Rec(2005)10 on "special investigation techniques" in relation to serious crimes including acts of terrorism, par 6.

[35] ibid. par 77 (*Association for Eurtopean Integration and Human Rights and Ekimdzhiev v. Bulgaria*, ECtHR judgment of 28 June 2007).

[36] See page 7 of the 2011 Report by the Research Division of the ECHR on "Internet: case-law of the European Court of Human Rights, available at http://www.echr.coe.int/Documents/Research_report_internet_ENG.pdf.

[37] See also CoE Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Strasbourg, 28 January 1981, Article 5, ratified by Ukraine on 30 September 2010 and entered into force on 1 January 2011, available at http://conventions.coe.int/Treaty/en/Treaties/Html/108.htm, and CoE Committee of Ministers, Recommendation R (87) 15E on regulating the use of personal data in the police sector, Strasbourg, 17 September 1987, available at https://wcd.coe.int/ViewDoc.jsp?id=704881&Site=CM. See also par 46 of the UN Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, Report to the UN Human Rights Council, 17 May 2010, A/HRC/14/46, available at http://www.un.org/Docs/journal/asp/ws.asp?m=A/HRC/14/46.

[38] *Op. cit.*, footnote 32, par 86 (*Association for Eurtopean Integration and Human Rights and Ekimdzhiev v. Bulgaria,* ECtHR judgment of 28 June 2007).

[39] ibid. par 90 (*Association for Eurtopean Integration and Human Rights and Ekimdzhiev v. Bulgaria*, ECtHR judgment of 28 June 2007).

investigative instruments that are provided in the CoE Cybercrime Convention[40] are included therein, coupled with adequate substantive and procedural safeguards (Article 15 par 2 of the CoE of the Cybercrime Convention). In that respect, while it is noted that certain of these investigative instruments are mentioned as the prerogatives of the (new) structural department for combatting cybercrime (see Article 5 par 4 of the Draft Law), the Draft Law does not provide the adequate substantive and procedural safeguards that are required according to Article 15 par 2 of the CoE Cybercrime Convention. Consequently, the reference to "acts to ensure immediate preservation of computer data or information flow data with regard to which there is a threat of destruction or damage" (corresponding to the measures mentioned in Title 2 of the CoE Cybercrime Convention) should be removed from Article 5 of the Draft Law and an equivalent provision introduced in the Criminal Procedure Code.

50. Finally, the Draft Law does not appear to deal with the creation of a body that would specialise in digital forensics (i.e. the branch of forensic science concerned with the recovery and investigation of material found in digital and computer systems)[41] - an indispensable element of successful investigations into cybercrime. Article 7 of the Draft Law refers generally to 24/7 assistance being provided for the investigation of cybercrime-related offences, but refers to this in a very vague manner, without mentioning such a separate entity/unit. The Criminal Procedure Code also does not seem to contain provisions relating to the identification, collection and analysis of electronic evidence through digital forensics.

51. Legal frameworks optimized for electronic evidence, together with law enforcement and criminal justice capacity to identify, collect and analyse electronic evidence, are central to an effective crime response, not only as regards cybercrimes but more generally for all crimes.[42] If not already provided in other legislation, it would be advisable to provide for the establishment of such a national digital forensic agency, employing specialized ICT experts, either in the Draft Law or in separate legislation; the CPC should also be supplemented as appropriate. This could for instance take the form of an expert center at the level of the police. Additionally, the Criminal Procedure Code should be supplemented with provisions relating to digital forensics, as well as electronic evidence and their lawful use before court, which should be consistent with the related legislation establishing such body. Adequate human and financial resources should also be allocated and capacity development initiatives implemented to ensure the proper and efficient functioning of such an entity.

4.4. Roles of NGOs, Enterprises, Individuals and Obligations of Service Providers

52. Article 4 of the Draft Law provides that the authorized body for combatting cybercrime (supposedly the entity to be established according to the last paragraph of the same Article 4) can decide that certain public bodies, but also

[40] See in particular the following provisions of the CoE Cybercrime Convention: Title 2 (Expedited preservation of stored computer data); Article 18 (Production order); Article 19 (Search and seizure of stored computer data); Article 20 (Real-time collection of traddic data); Article 21 (Interception of content data).

[41] *Op. cit.*, footnote 18, page 159 (2013 UNODC Comprehensive Stury on Cycercrime).

[42] ibid. page 157 (2013 UNODC Comprehensive Stury on Cycercrime).

"enterprises, institutions and organizations regardless of subordination and ownership form, their officials, as well as citizens *upon their consent*" may be involved in operations aimed at combatting cybercrime in accordance with the provisions of the Draft Law. It is understood that this condition of "consent" applies only to citizens and not to all the non-governmental entities listed in this provision. In order not to be overly burdensome on non-governmental actors, the provision should be clarified to ensure that such involvement is not an obligation and that co-operation with these entities occurs only on a voluntary basis.

53. Articles 6 and 9 of the Draft Law both relate to the interaction of entities in the field of preventing and combating cybercrimes. Though worded slightly differently, they appear to be identical in content and thus duplicate one another; one of the two provisions should therefore be deleted.

54. These Articles envisage a duty of service providers, NGOs and other civil society agents to co-operate with the competent bodies in preventing and combating cybercrimes. Additionally, Article 10 of the Draft Law requires that state bodies, local self-government, unions of citizens, organizations and their officials support the institutions which combat cybercrime by providing information and data related to cybercrimes. Certain of the activities envisioned, particularly relating to education, awareness-raising, capacity development and development of tools and protocols, are particularly important for achieving greater cybersecurity (see par 19 *supra*). However, it is overly burdensome to impose a duty on these various non-governmental actors to co-operate in these areas and it is recommended that the Article 6 (or 9) be amended to clarify that such co-operation occurs on a voluntary basis.

55. Furthermore, these provisions may impose an unreasonable burden on the said actors as they also refer to activities conducted for the "[re]solution of crimes and discovery of perpetrators" and provisions of information and data relating to cybercrimes. Within the framework of criminal investigations, such co-operation could be possible, but only if necessary for a particular criminal investigation, in a specific case and for a limited time, and not as a general duty.[43] It would, therefore, be advisable to delete in Article 6 (or 9) of the Draft Law the reference to the "[re]solution of crimes and discovery of perpetrators" and delete Article 10 of the Draft Law altogether. Such issues would be better addressed through criminal procedure rules and should be included in the Criminal Procedure Code.

56. Article 12 of the Draft Law also imposes a number of obligations on service providers. These include *inter alia* "informing the competent bodies about information flows, including illegal access to information from computer systems, attempts to introduce illegal software" (Article 12 par 1 (b)) and providing for "monitoring, surveillance and preservation of data flows for the identification of the providers of services, their users and the channel by which the message was transmitted, for a term of 360 calendar days" (Article 12 par 1 (f)).

57. It is positive that the provisions of Article 12 of the Draft Law (read together with the definition of "user data" of Article 1) seem to exclude the recording,

[43] See Article 15 par 2 of the CoE Cybercrime Convention.

retention and/or communication to the competent authorities of the *content* of information/communications, which is overall in line with international standards.[44]

58. However, the question of the service providers' obligations constitutes one of the most significant issues related to the exercise of the freedom of expression on the Internet. It must be pointed out that the UN Human Rights Committee has considered that any restriction on the operation of information dissemination systems, including that of internet service providers, is not legitimate unless it conforms with the test for restrictions on freedom of expression under international law.[45] The UN Special Rapporteur on Freedom of Opinion and Expression also noted how important it is for States to be transparent about the use and scope of communications surveillance techniques and powers, particularly when dealing with internet service providers.[46]

59. The CoE Cybercrime Convention requires State Parties to introduce new investigative measures (see par 49 *supra*) which are closely related to the obligations mentioned in Article 12 of the Draft Law. However, the CoE Cybercrime Convention measures are exclusively envisioned for the purpose of specific criminal investigations or proceedings, i.e., *a posteriori*. The measures contemplated by Article 12 of the Draft Law actually provide for a systematic collection and retention of certain data *a priori*, outside of any criminal investigation context.

60. It must be noted in that respect that the EU Directive 2006/24/EC[47] which contained a similar obligation for the systematic retention by service providers of certain data (e.g., traffic data, data flows for the identification of the providers of services and their users, etc.) was recently declared invalid for violating Articles 7 and 8 of the Charter of Fundamental Rights of the European Union (respectively on the right to respect for private and family life and the right to protection of personal data).[48] To reach such a conclusion, the Court of Justice of the European Union (hereinafter "CJEU") noted in particular the following:

- that retention measures were applied even to persons for whom there was no evidence capable of suggesting that their conduct might have a link with a serious crime;[49]

---

[44] See e.g., the CoE Committee of Ministers Declaration on freedom of communication on the Internet, 28 May 2003, available at http://www.coe.int/t/informationsociety/documents/Freedom%20of%20communication%20on%20the%20Internet_en.pdf.

[45] See par 43 of the UN Human Rights Committee, General Comment No. 34 on Freedom of Opinion and Expression , 12 September 2011, available at http://www2.ohchr.org/english/bodies/hrc/docs/gc34.pdf.

[46] See pars 91-92 of the 2013 Report of the UN Special Rapporteur on Freedom of Opinion and Expression available at http://www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session23/A.HRC.23.40_EN.pdf.

[47] Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC.

[48] See pars 58 to 69 of the Judgment of the Court of Justice of the European Union, *Digital Rights Ireland Ltd v. Ireland*, 8 April 2014, C-293/12, available at http://curia.europa.eu/juris/document/document.jsf?text=&docid=150642&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=265234.

[49] ibid, par 58 (CJEU C-293/12 *Digital Rights Ireland Ltd v. Ireland*).

- that it did not provide for any exception, with the result that it applied even to persons whose communications were subject, according to rules of national law, to the obligation of professional secrecy;[50] and
- that there was no need to demonstrate any relationship between the data whose retention was provided for and a threat to public security.[51]

61. As regards access by the competent national authorities to the said data and their subsequent use, the CJEU further pointed out, amongst others, the failure to lay down any objective criterion by which to determine the limits for granting such access and determining their subsequent use,[52] as well as the lack of substantive and procedural safeguards to prevent undue access and use by the national authorities.[53] Regarding the duration of detention (between 6 to 24 months), the CJEU considered that the determination of the period of retention should have been based on objective criteria in order to ensure that it was limited to what was strictly necessary.[54] In light of the above, the CJEU concluded that systematic retention of data by internet service providers, without being precisely circumscribed by provisions to ensure that it is actually limited to what is strictly necessary, constituted a disproportionate interference with fundamental rights and freedoms.

62. As it is drafted, Article 12 of the Draft Law does not seem to be equipped with adequate safeguards and does not appear to adhere to the above-mentioned principles. This provision provides systematic data retention outside of any criminal investigation, without any limitations as to the material and personal scope and without providing the necessary substantive and procedural safeguards to ensure that the public authorities only access and use the said data if this is necessary in the context of criminal investigation. A practice involving such broad and systematic data retention may lead to undue interference with the rights to respect for private life and to data protection.[55] It is therefore recommended to delete the obligations prescribed by Article 12 of the Draft Law.

63. Instead, such investigative measures should be included under the Criminal Procedure Code in the context of criminal investigations and coupled with adequate substantive and procedural safeguards similar to the ones detailed in pars 44-48 *supra*. Given the need for expedited measures in the context of cybercrime, it would be important for the Criminal Procedure Code to also provide for fast-track procedures in that respect.

64. Article 12 par 1 (b) of the Draft Law requires service providers to provide information relating to cases of "illegal access to information from computer

---

50 ibid, par 58 (CJEU C-293/12 *Digital Rights Ireland Ltd v. Ireland*).
51 ibid, par 59 (CJEU C-293/12 *Digital Rights Ireland Ltd v. Ireland*).
52 ibid, par 60 (CJEU C-293/12 *Digital Rights Ireland Ltd v. Ireland*).
53 ibid, pars 61-62 (CJEU C-293/12 *Digital Rights Ireland Ltd v. Ireland*).
54 ibid, par 64 (CJEU C-293/12 *Digital Rights Ireland Ltd v. Ireland*).
55 See also CoE Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Strasbourg, 28 January 1981, Article 5, ratified by Ukraine on 30 September 2010 and entered into force on 1 January 2011, available at http://conventions.coe.int/Treaty/en/Treaties/Html/108.htm, and CoE Committee of Ministers, Recommendation R (87) 15E on regulating the use of personal data in the police sector, Strasbourg, 17 September 1987, available at https://wcd.coe.int/ViewDoc.jsp?id=704881&Site=CM. See also par 46 of the UN Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, Report to the UN Human Rights Council, 17 May 2010, A/HRC/14/46, available at http://www.un.org/Docs/journal/asp/ws.asp?m=A/HRC/14/46.

systems" and "attempts to introduce illegal software". This should not be interpreted as a requirement to conduct constant monitoring of all communications over the providers' network, or to detect such illegal conduct, as this would constitute an unreasonable and costly burden for them.[56] In principle, no general obligation to monitor or seek facts or circumstances indicating illegal activity should be imposed on service providers.[57] The Law should only provide for an obligation for subsequent action or control, once they are aware of the illegal nature of the content. In that respect, the provisions of the EU Directive on electronic commerce (2000/31/EC),[58] though not binding in Ukraine, could serve as useful guidance. According to its provisions, service providers should not be liable for the content posted by the third party on condition that they: (a) do not have actual knowledge of illegal nature of the content or (b) upon obtaining such knowledge or awareness, they act expeditiously to remove or to disable access to the unlawful content.[59]

65. Finally, in order to ensure that effective criminal investigations can be carried out to identify and prosecute a perpetrator, the legal framework should allow the police or the courts, subject to adequate guarantees and safeguards, to request internet service providers to reveal the identity of the person who has posted some content which constitutes a crime or violates the rights and freedom of others (e.g., child's right to respect for his private life and protection from physical and mental integrity).[60] In that context, anonymity and confidentiality on the Internet must not lead States to refuse to protect the rights of potential victims, especially where vulnerable persons are concerned.[61] If needed, the Criminal Procedure Code should be supplemented to that effect.

5. Restrictions of Access to Information

66. Article 13 of the Draft Law provides for the possibility to "suspend the work of the network and (or) communication means, the provision of communications services, access to internet resources and (or) information located thereon". Such measures may be applied in cases of information provided by state and local authorities, organizations or citizens in "which is provided in violation of the current law, contains appeals to mass riots, conduction of extremist activities, participation in mass (public) activities conducted in violation of the established order, […] use of networks and (or) communication means with criminal goals, which harm the interests of a person, the society and the state, and the dissemination of information which violates the legislation on elections

---

[56] This seems to be mirroring certain of the obligations provided under Article 13 of the EU Framework Directive 2009/140/EC of 25 November 2009, available at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:337:0037:0069:EN:PDF, that includes an obligation for EU member States to ensure the integrity and security of public communications networks and publicly available communications services as well as the continuity of such services.

[57] See also *op. cit.*, footnote 44, Principle 6 (2003 CoE Committee of Ministers Declaration on freedom of communication on the Internet). See also the Judgment of the Court of Justice of the European Union, *Scarlet Extended SA v Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)*, 24 November 2011, C-70/10, available at http://curia.europa.eu/juris/liste.jsf?language=en&num=C-70/10.

[58] See also, for reference, though not binding on Ukraine, the Directive 2000/31/EC of the European Parliament and the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (hereinafter "the 2000 Directive on electronic commerce"), available at http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32000L0031.

[59] ibid., Articles 12 to 14 (2000 Directive on electronic commerce).

[60] *Op. cit.*, footnote 12, par 49 (*K.U. v. Finland*, ECtHR judgment of 2 December 2008).

[61] *Op. cit.*, footnote 36, page 24 (2011 Report by the ECHR on Internet and ECHR case-law).

in Ukraine".

67. First of all, Article 13 of the Draft Law raises concerns with regard to Article 10 of the ECHR, Article 19 of the ICCPR, as well as par 9.1 of the OSCE Copenhagen Document, which protect the right to freedom of expression and information. The ECtHR has noted that "the right to internet access is considered to be inherent in the right to access information and communication protected by national Constitutions, and encompasses the right for each individual to participate in the information society and the obligation for States to guarantee access to the Internet for their citizens. It can therefore be inferred from all the general guarantees protecting freedom of expression that a right to unhindered Internet access should also be recognized".[62] Additionally, the Human Rights Committee highlighted that "[g]iving effect to the right to freedom of expression imposes an obligation on States to promote universal access to the Internet. Access to the Internet is also necessary to promote respect for other rights, such as the […] right to assembly and association". It must be pointed out that denying individuals the right to access the Internet is an extreme measure that could be justified only as a last resort, and based on a court decision.[63]

68. Article 13 of the Draft Law allows the State to restrict access to information and the Internet in the above-mentioned cases, which are vaguely formulated and potentially open to a wide range of interpretations. In particular, Article 13 refers to the "conduct of extremist activities" which is a vague term not further defined by the Draft Law. In line with the ECtHR requirements that laws need to be precise and foreseeable, the UN Human Rights Committee has noted that offences relating to "extremist activity" should be clearly defined to ensure that they do not lead to unnecessary or disproportionate interference with the freedom of expression.[64] In this respect, both the CoE Committee of Ministers' Guidelines on Protecting Freedom of Expression and Information in Times of Crisis (2007)[65] and the OSCE/ODIHR Manual on "Countering Terrorism, Protecting Human Rights" (2007)[66] caution against the imposition of undue restrictions on the exercise of freedom of expression and assembly during crisis situations.

69. It must be pointed out that freedom of expression includes the right to impart, seek and receive information, as well as to hold opinions. It is applicable "not only to information or ideas that are favourably received or regarded as inoffensive or as a matter of indifference, but also to those that offend, shock or disturb the State or any sector of the population".[67] While the threshold for

---

62 See par 31 of *Yildirim v. Turkey*, ECtHR judgment of 18 December 2012 (Application No 3111/10), available at http://hudoc.echr.coe.int/sites/fra/pages/search.aspx?i=001-115705#{"itemid":["001-115705"]}.

63 See par 6 (c) of the 2011 Joint Declaration on Freedom of Expression and the Internet by the UN Special Rapporteur on Freedom of Opinion and Expression, the OSCE Representative on Freedom of the Media, the Organization of American States (OAS) Special Rapporteur on Freedom of Expression and the African Commission on Human and Peoples' Rights (ACHPR) Special Rapporteur on Freedom of Expression and Access to Information, 1 June 2011, available at http://www.oas.org/en/iachr/expression/showarticle.asp?artID=848&lID=1.

64 See par 46 of UN Human Rights Committee General Comment No. 34.

65 Adopted by the Committee of Ministers on 26 September 2007 at the 1005th meeting of the Ministers' Deputies, available at https://wcd.coe.int/ViewDoc.jsp?id=1188493.

66 Particularly, see Chapter 16 "Freedom of Association and the Right to Peaceful Assembly", pages 240-250 available at http://www.osce.org/odihr/29103?download=true.

67 See par 49 of *Handyside v. United Kingdom*, ECtHR judgment of 7 December 1976 (Application No 5493/72). See also par 11 of the Human Rights Committee General comment No. 34, available at

interference with the right is high, this freedom is not absolute. It may be restricted by the state, in line with international human rights standards, where it is abused to violate another person's rights or where it poses a serious risk to the public order (for example, through the incitement to, or advocacy of, violence against others; the promotion of racial or religious hatred; or the intentional communication and direct incitement to the commission of a terrorist act).[68]

70. Nevertheless, any measure taken to restrict this right should be strictly proportionate to the threat and fulfil the requirements described above. In a democratic society, the state has to tread carefully in order to preserve the rights and freedoms of those who peacefully pursue a political agenda, albeit a radical or even extreme one. The expression of radical or extremist views that do not involve the incitement to commit criminal acts should not be criminalized or restricted. Any discretionary powers afforded to law enforcement officials should be narrowly framed and include adequate safeguards to reduce the potential for arbitrariness. Any pre-emptive measures should be transparent and based on corroborated evidence, have time limits and be subject to independent or judicial review. As regards efforts to prevent terrorist radicalization on the Internet more specifically (such as regulating, filtering or blocking online content deemed to be illegal under international law), restrictions should be in compliance with international human rights standards and made according to the rule of law, so as not to impact unlawfully on the freedom of expression and the free flow of information. Security measures should be temporary in nature, narrowly defined to meet a clearly set-out legitimate purpose and prescribed by law. These measures should not be used to target dissent and critical speech.[69] The pre-emptive measures contained in Article 13 of the Draft Law do not seem to fulfil such requirements.

71. Second, Article 13 refers to "appeals to mass riots" and to "participations in mass (public) activities conducted in violation of the established order". Article 11 of the ECHR, Article 21 of the ICCPR and par 9.2 of the OSCE Copenhagen Document protect the right to freedom of peaceful assembly. In principle, there exists a presumption in favour of holding assemblies[70] and a presumption of peaceful intent in favour of this freedom should likewise prevail. According to Article 11 par 2 of the ECHR, any restrictions to this right should be prescribed by law and be necessary in a democratic society in the interests of national security or public safety, 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.

---

http://www2.ohchr.org/english/bodies/hrc/docs/GC34.pdf, which states that "[t]he scope of paragraph 2 [of Article 19 of the ICCPR] embraces even expression that may be regarded as deeply offensive".

68 See the definition of "incitement to terrorism" provided on page 22 of the 2010 Report of the UN Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, A/HRC/16/51, 22 December 2010, available at http://www2.ohchr.org/english/bodies/hrcouncil/docs/16session/A-HRC-16-51.pdf, which reads as follows: "it is an offence to intentionally and unlawfully distribute or otherwise make available a message to the public with the intent to incite the commission of a terrorist offence, where such conduct, whether or not expressly advocating terrorist offences, causes a danger that one or more such offences may be committed".

69 See the OSCE Study "Freedom of Expression on the Internet: A study of legal provisions and practices related to freedom of expression, the free flow of information and media pluralism on the Internet in OSCE participating States" (2010) by the OSCE Representative on Freedom of the Media, available at http://www.osce.org/fom/80723.

70 See Principle 2 of the OSCE/ODIHR-Venice Commission Guidelines on Freedom of Peaceful Assembly, Second Edition (2010), available at http://www.osce.org/odihr/73405?download=true.

72. Restrictions imposed prior to an assembly can only be justified on the basis of legitimate grounds, as established by international and regional human rights instruments. In particular, restrictions based on public-order grounds should not be imposed where there is only a hypothetical or unsubstantiated risk of public disorder or due to the mere presence of a hostile audience, all of which are not legitimate grounds for prohibiting a peaceful assembly.[71] Prior restrictions imposed on the basis of the possibility of minor incidents of violence are also likely to be disproportionate, and any isolated outbreak of violence should be dealt with by way of subsequent arrest and prosecution rather than prior restraints imposed on the assembly as such.[72] In this respect, due to its broad restriction of access to information, Article 13 of the Draft Law is not compliant with international human rights standards.

73. Additionally, Article 13 of the Draft Law may potentially have an impact on the right to freedom of association since the blocking of internet websites or certain sources of information or communication tools can have a significant negative impact on associations.[73] It may thus amount to a disproportional interference with the exercise of the afore-mentioned right, which should be subject to the same principles of proportionality and 'necessity in a democratic society' as limitations to freedom of peaceful assembly.[74]

74. Bearing all of the above in mind, it is noted that Article 13 of the Draft Law is formulated too vaguely and too broadly to satisfy the requirement of foreseeability enshrined in international and regional human rights standards. This provision could thus lead to unnecessary and disproportionate limitations of the freedoms of peaceful assembly, freedom of association and freedom of expression. It is thus recommended to remove from Article 13 of the Draft Law references to the grounds justifying limitation to the use and access to the Internet/ICTs which are not in line with international standards and consider replacing them by a list of 'legitimate' grounds according to international standards (e.g., incitement to violence against others; the promotion of racial or religious hatred; the intentional communication and direct incitement to the commission of a terrorist act; child pornography-related acts).

75. Article 13 provides that decisions to block access to information or the Internet lies with the National Commission for Protection of Information and Information Technologies. More specifically, this National Commission may request communication operators to suspend access to the information resource, including to a website, within one hour of the request (Article 13 pars 1 and 4). The Commission can also request the hosting provider to take action to delete

---

71 ibid. par 71 (2010 Guidelines on Freedom of Peaceful Assembly). See also *Makhmudov v. Russia*, ECtHR judgment of 26 July 2007 (Application No 35082/04), available at http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-81966.

72 See par 94 of *Stankov and the United Macedonian Organisation Ilinden v. Bulgaria*, ECtHR judgment of 2 October 2001 (Application No 29221/95), available at http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-59689#{"itemid":["001-59689"]}.

73 See par 47 of *Socialist Party v. Turkey*, ECtHR judgment of 25 May 1998 (Application No 21237/93), available at http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-58172#{"itemid":["001-58172"]}.

74 See 2013 Report by Ian Brown, "Report on Online Freedom Expression, Assembly and Association and the Media in Europe", MCM(2013)007, available at http://www.coe.int/t/dghl/standardsetting/media/belgrade2013/Online%20freedom%20of%20expression,%20assembly,%20association_MCM(2013)007_en_Report_IanBrown.pdf, which states that "blocking access to associations websites, and communications tools such as webmail and social networking sites, can have a significant negative impact on assembly and association".

the allegedly illegal data/content; in that case, the hosting provider should contact the servicing owner within three hours of the request to ask for immediate removal of the allegedly illegal data/content.

76. The Commission is a collegial body which is explicitly stated to be "subordinated to the President of Ukraine" and also under the influence of other executive bodies such as the Ministry of Internal Affairs and the Ministry of Defense. In that respect, it appears that the composition and organizational structure of the body in charge of deciding on restrictions of access to information and internet access is under a strong influence of the executive and that there is no system of supervision by an independent entity. As previously mentioned, given the seriousness of the measure, the decision to block internet access should be a decision imposed by a court, following appropriate court procedures.[75] Additionally, the restrictions to the use and access to the Internet decided by the court should be strictly limited to what is necessary. The restriction should not amount to a general suspension of the network or general prohibition to use and access the Internet and ICTs and the court should always examine whether there are less far-reaching measures which could be taken.[76]

77. As for the Commission, it is recommended to replace its powers listed under Article 13 with more general powers (e.g., monitoring of *public* networks for identification of alleged criminal offences, receiving notifications of suspicion of illegal content by individuals, notifying the Prosecutor General of suspicion of illegal content).[77] The Prosecutor General could then submit a petition to the court to request the blocking of the access to the page containing illegal content and deletion of such content. Then, on the basis of the court judgment acknowledging the illegality of the content and ordering temporary suspension of access as well as the deletion of illegal content, the National Commission could be in charge of ensuring the implementation of the suspension orders and deletion of illegal data, including liaising with communications operators and hosting providers to request implementation (e.g., blocking access and deletion of illegal content).

78. In light of the above, Article 13 of the Draft Law should also be amended to specify that the Prosecutor General shall apply to a court to request such restrictive measures, in accordance with the provisions of the Criminal Procedure Code. Consequently, the Code of Criminal Procedure should be supplemented to that effect. The drafters could also consider introducing fast-track procedures.

79. Finally, it is noted that Article 13 of the Draft Law does not clearly state the rules and procedures relating to the nomination and appointment of the National Commission's members, including the representatives of the media and of the public, nor does it provide for overarching principles that should guide its functioning and decision-making. Even if not all the details need to be expressly

---

[75] *Op. cit.*, footnote 63, par 6 (c) (2011 UN-OSCE-OAS-ACHPR Joint Declaration on Freedom of Expression and the Internet). See also UN Human Rights Committee, General Comment 34 on Freedom of Opinion and Expression, available at http://www2.ohchr.org/english/bodies/hrc/docs/gc34.pdf.

[76] See *Ahmet Yildirim v. Turkey*, ECtHR judgment of 18 December 2012 (Application No 3111/10).

[77] See e.g., though in the context of copyrights infringements, pages 673 and 674 of the Article on "Access to Network Services and Protection of Constitutional Rights: Recognizing the Essential Role of Internet Access for the Freedom of Expression", Cardozo Journal of International and Comparative Law (2011, Vol. 19), available at http://www.cjicl.com/uploads/2/9/5/9/2959791/cjicl_19.3_lucchi_article.pdf.

stated, at least the basic principles should be laid down in the Draft Law, which should then also refer to secondary legislation to be adopted to further elaborate these aspects. Regulations on nomination and appointment of members should be crafted so as to ensure gender-balanced representation.[78]

80. Articles 14 and 16 of the Draft Law provide for some forms of compensation for damages to be paid to the victims by the perpetrator of cybercrime. However, the draft legislation does not provide for the possibility to bring a claim against public authorities to seek redress for interferences with privacy or related rights as the result of undue use of secret surveillance measures as those contemplated by the Draft Law.

6. International Co-operation and Liability

81. Article 19 of the Draft Law regulates the handling of a request of a foreign state to receive information related to combating of cybercrime. The purpose of this Article seems to be to transpose a number of provisions of the CoE Cybercrime Convention pertaining to such requests. However, a number of observations should be made in this respect.

82. First, Article 19 par 1 of the Draft Law stipulates that "Ukraine shall provide information on issues connected with combating cybercrime to a foreign state based on an application, while observing the requirements of Ukrainian law and its international and legal obligations". It should be noted that this provision does not mention the possibility for spontaneous information of other State parties (as per Article 26 of the CoE Cybercrime Convention), provided that certain safeguards are in place; such spontaneous information does not require a prior request for information.

83. Second, Article 19 par 2 of the Draft Law determines that expedited preservation of data may be requested by other countries from Ukrainian authorities. However, Article 19 par 2 of the Draft Law does not provide the Ukrainian authorities with the power to actually request another State Party to order or obtain the expedited preservation of data. Moreover, the provisions of the Criminal Procedure Code do not seem to provide for such coercive measures. As recommended in par 49 *supra*, the Criminal Procedure Code should be supplemented to that effect.

84. Third, the provision fails to specify the stipulation prescribed by Article 29 par 3 of the CoE Cybercrime Convention which states that "dual criminality shall not be required as a condition to providing such preservation".

85. Fourth, the provision does not spell out the specific instances when a request may be refused. These instances are envisaged by Article 29 pars 4 to 7 of the CoE Cybercrime Convention and include *inter alia* cases where the request concerns an offence which the requested party considers a political offence, or where the party believes that preservation will not ensure the future availability of the data etc. Such omission does not provide Ukraine with the legal grounds

[78] See pars 9-10 of the Appendix to the Recommendation Rec (2003)3 of the Committee of Ministers to CoE Member States on the balanced participation of women and men in political and public decision-making adopted on 30 April 2002, available at https://wcd.coe.int/ViewDoc.jsp?id=2229, which states that the Member States should provide for gender-balanced representation in all appointments made by a minister or government to public committees and in posts or functions whose holders are nominated by government and other public authorities.

for refusing the request under certain circumstances.

86. Fifth, Article 19 par 4 of the Draft Law provides for a term of 60 days for the preservation of data. It should be noted that Article 16 par 2 of the CoE Cybercrime Convention stipulates that the "Party shall adopt such legislative and other measures as may be necessary to oblige that person to preserve and maintain the integrity of computer data for a period of time as long as necessary, up to a maximum of ninety days, to enable the competent authorities to seek its disclosure. A Party may provide for such an order to be subsequently renewed". The CoE Cybercrime Convention further prescribes conditions and safeguards for such renewal which shall, *inter alia*, "include judicial or other independent supervision, grounds justifying application, and limitation of the scope and the duration of such power or procedure". Such possibility for renewal, as well as conditions and safeguards are not included in Article 19 of the Draft Law nor do they seem to be available in the Criminal Procedure Code. As previously mentioned, such provisions should rather be provided under the Criminal Procedure Code and not in the Draft Law

87. Finally, the last paragraph of Article 19 states that "the transfer of computer data is carried out only after the acceptance by a competent body of Ukraine of a request on the provision of international legal assistance in the field of criminal law". It should be noted that this provision only concerns the transfer of the preserved data but does not mention its preservation.

88. In light of all of the above and in order to ensure the appropriate transposition of the relevant CoE Cybercrime Convention provisions, it would be advisable to revise and supplement Article 19 of the Draft Law in the manner set out above, except for those provisions which should be included under the Criminal Procedure Code.

89. Article 22 of the Draft Law states that "the violation of this law entails disciplinary, civil, administrative or criminal responsibility of Ukraine" without referring to any specific legal provisions. It is not clear what type of liability (disciplinary, criminal, administrative, or civil) will apply to the violation of which provisions of the Draft Law. As it now stands, this provision is very vague. Generally, it would be helpful for persons affected by, and entities applying the law to know what type of behaviour would constitute a violation of the law and what would be the consequences of such violations. This should be specified in the Draft Law, and cross-references to other pertinent legislation should likewise be included.

[END OF TEXT]

ANNEX – Draft Law of Ukraine on Combating Cybercrime

Draft

LAW OF UKRAINE
On Combatting Cybercrime

This Law establishes the legal and organizational basis for combatting **cybercrime,** discovering and eliminating the reasons and conditions which cause these crimes, interacting in order to prevent and combat crime in the field of computer technologies, protecting and providing assistance to service providers and users of computer systems, cooperating with other national, international and regional organizations in this field.

The provisions of this Law may not be used as a basis for prosecuting citizens who act within the boundaries of the law to protect their constitutional rights and freedoms.

Chapter I
GENERAL PROVISIONS

Article 1. Main definitions

This Law uses the following main definitions:

cybercrime – criminal activity, connected with the use of computers, information technologies, global networks and cyberspace;

cyber-crime – is a guilty socially dangerous penal act committed by using computer technologies and intrusion upon the work of computers, software, computer networks, unsanctioned modification of computer data, as well as other illegal socially dangerous acts committed using or with the assistance of computers, computer networks and software, and using or with the assistance of other devices to gain access to the computer-modeled information space.

cyberspace – computer-modeled information space containing data on persons, objects, facts, events, phenomena and processes, represented in mathematical, symbol or any other form, which circulate over local or global computer networks, or data

contained in the memory of any physical or virtual device or any other media specially designed for its storage, processing and transfer, a unique space which is not located in geographical space but is accessible in any part of the world through access to the Internet.

cyber stalking – a form of electronic stalking most often involving clearly manifested or imaginary physical threats creating a feeling of danger with the victim;

hacking – use of Internet-technologies in order to hack computer networks and their users;

hacktivism – crimes aimed at breeching the confidentiality of data – illegal access to computers and computer systems without harming the data;

destructive cybercrimes – crimes which consist in compromising data and encroaching on data integrity and the secure functioning of computer systems;

cyber theft and cyber fraud – crimes connected with the use of computer technologies which encroach on property, ownership rights, ownership rights to information, and copyright;

These crimes also include ***– illegitimate assignment,*** *which differs from embezzlement in the way that the criminal was not entrusted with the valuables, but having access to the system he/she changed the documents in a way to acquire ownership rights to property which should not belong to him/her.*

Corporate (industrial) espionage*, when the employees of an enterprise or other persons use computers and networks to steal commercial secrets (for example, the recipe of a beverage, manufactured by a competitor). The object of theft may also be financial data, confidential client lists, marketing strategies or any other information which may be used to subvert the business or receive a competitive advantage.*

Plagiarism *– theft of copyright materials with their further publication as one's own.*

Piracy *– illegal copying of copyright-protected software, as well as music, movies, books and other works of art resulting in losses for the legal copyright holder.*

Personal data theft*, when the Internet is used to receive personal*

data on the victim, for example, the number of his/her driver's license, credit card and bank account numbers for further fraud, including gains of money and property with the help of personal data.

Theft and further illegal changes of DNS (domain name server) data.

cyber trafficking – transfer of illegal intellectual commodities, software, and encryption technologies prohibited in certain states via the Internet;

computer system – any device or collection of interconnected or joint devices, one or more of which automatically processes data based on a certain program;

computer data – any representation of facts, information or concepts in a form usable for processing by a computer system, including software designed for the performance of various actions by the computer system;

service provider – any state or private entity which provides the users with the possibility to exchange data via a computer system, as well as any other entity which processes or stores computer data as authorized by the communication service or the users of its services;

data on information flows – any data connected with operations involving the transfer of data with the help of a computer system, generated by a computer system, which is a link in the respective chain of communications, and indicates the source, designation, route, time, date, size, duration or type of the respective network service;

user data – any information on its subscribers available with the service provider in the form of computer data or any other form, with the exception of data on the flows or content of information, using which it is possible to identify: the type of communications service used, the technical activities taken with regard to it, and the duration of the provision of the service; the identity of the user, his/her geographical address, home telephone number or any other contact telephone number, information on accounts charged and payments made, personal data in the service agreement or contract; any other data on the location where the communications equipment has been installed which is

available in the service agreement or contract, as well as any other data which may lead to the identification of the user;

security measures – the application of procedures, devices or specialized computer software in order to restrict or prohibit the access of certain types of users to the computer system.

Article 2. Main principles for preventing and combatting crime in the field of computer technologies

Prevention and combatting crime in the field of computer technologies is based on the following principles:

a) legality;

b) observation of fundamental rights and freedoms of a human being;

c) swift response;

d) inevitability of punishment;

e) computer security and protection of personal data;

f) inclusive use of prophylactic measures: legal, social, economic and informational;

g) social partnership, cooperation between public governance authorities and international organizations, NGOs and other civil society agents.

Article 3. Crimes, included into the definition of cybercrime

Cybercrime includes the following crimes connected with the use of computer technologies:

- violent or other potentially dangerous cyber crimes, which encroach on the physical security, life or health of a person;

- cyber theft and cyber fraud;

- cyber stalking;

- destructive cyber crimes;

- use of Internet technologies in order to harm computer networks and their users;

- crimes connected with the use of computer technologies

which encroach on public morals;

- crimes connected with the use of computer technologies which encroach on public safety;

- hacking;

- hacktivism;

- other cyber crimes – crimes, which are committed with the help of computer networks and which encroach on various subjects protected by the law.

Traditional crimes, committing which is facilitated by the computer, or for which the use of a computer opens new opportunities – *these are in the first place the following:*

- ***advertisement of prostitution services*** *over the network;*

- ***illegal circulation of drugs*** *using the Internet;*

- ***gambling games on the Internet****;*

- ***money laundering*** *through electronic transfer;*

- ***cyber trafficking****, or the transfer of illegal commodities, such as encryption technologies prohibited in certain states, over the Internet.*

Chapter II

ORGANIZATIONAL BASIS FOR COMBATTING CYBERCRIME

Article 4. Subjects of combatting cybercrime

The Cabinet of Ministers of Ukraine within its competence organizes the combat with cybercrime and Ukraine and provides for the necessary forces, means and resources.

The central executive authorities participate in combatting cybercrime within their competence, which is established by the laws and other legal acts issued based on them.

The subjects who directly participate in combatting cybercrime within their field of competence are:

The Ministry of Internal Affairs of Ukraine – the main body in the national system for combatting cybercrime;

The Security Service of Ukraine;

The Ministry of Defense of Ukraine;

Other central executive authorities which provide for and implement state policy in the field of computer technologies.

When necessary, the central and local executive and self-governance bodies, which operate in the field of computer technologies and use computer networks, participate in the activities connected with the prevention, discovery and termination of cybercrime.

By decision of the management of the authorized body for combatting cybercrime, other central and local executive and self-governance bodies, enterprises, institutions and organizations regardless of subordination and ownership form, their officials, as well and citizens upon their consent may be involved in the operations aimed at combatting cybercrime in accordance with the requirements of this Law. **The coordination of the activities of the subjects involved in combatting cybercrime and of the use of new technologies in countering cyber-attacks is carried out by a separate structural department for combatting cybercrime of the Ministry of Internal Affairs of Ukraine.**

As an option (The coordination of the activities of the subjects involved in combatting cybercrime and of the use of new technologies in countering cyber-attacks is carried out by the National Center for Combatting Cybercrime.

The National Center for Combatting Cybercrime is a state body subordinated and reporting to the Ministry of Internal Affairs of Ukraine and is established as part of implementation of this Law by the Cabinet of Ministers using the staff and based on the Department for Combatting Corruption of the Ministry of Internal Affairs of Ukraine.)

Article 5. Authority of competent state bodies and institutions in prevention and combatting crime in the field of computer information.

The Ministry of Internal Affairs and its structural departments carry out special investigative activities, criminal prosecution, international cooperation and identification of persons who have committed crimes falling under their competence in the field of

computer technologies, coordinates, manages and carries out criminal prosecution under the process provided by the law.

The Security Service of Ukraine and its structural departments carry out special investigative activities, criminal prosecution, international cooperation and identification of persons who have committed crimes falling under their competence in the field of computer technologies.

The Ministry of Defense of Ukraine in order to provide for the defense capability of the state carries out special activities in the field of prevention, discovery and termination of threats which involve the use of computer technologies;

The structural department for combatting cybercrime of the Ministry of Internal Affairs prepares and recurrently updates databases on criminal activities involving computer technologies, implements measures to prevent and combat crime in the field of computer information which poses a threat to national security, conducts investigative and search activities, takes action to discover the connections of international criminal organizations, as well as within the scope of criminal prosecution under the application of a prosecutorial body or upon its own initiative, acts to ensure immediate preservation of computer data or information flow data with regard to which there is a threat of destruction or damage, takes action in accordance with the criminal procedure law, implements other activities within its competence in these issues.

The National Commission for State Regulation in the Field of Communication and Information (NCRCI) jointly with the **structural department for combatting cybercrime** of the Ministry of Internal Affairs submits proposals on protection and security of computer data.

The Kharkiv National University of Internal Affairs shall provide for the professional training and development of staff involved in combatting computer crimes.

Article 6. Interaction of competent bodies in the field of preventing and combatting crime involving the use of computer technologies

Under the framework of the activities for prevention and combatting crime in the field of computer technologies the competent bodies, service providers, NGOs and other civil society agents shall cooperate via exchange of information and expertise, through the conduction of joint activities aimed at the solution of crimes and the discovery of perpetrators, personnel training, development of initiatives aimed at the implementation of programs, practices, activities, procedures, minimal computer system security standards, organization of campaigns for informing about computer crimes and the risks which the users of computer systems face, as well as conduct other activities in this field.

Article 7. Authority of subjects, directly involved in combatting cybercrime

The Ministry of Internal Affairs:

combats cybercrime through the implementation of investigative and search activities aimed at the prevention, discovery and termination of crimes involving the use of computer technologies, including international;

collects information on the activities of criminal organizations which commit crimes using computer technologies;

provides on a 24/7 basis urgent assistance to the investigation or prosecution with regard to criminal offences connected to computer systems and data, or the collection of electronic evidence which applies to the criminal offence;

provides qualified personnel and respective equipment for ensuring 24/7 urgent assistance and the support of the operations of this network.

acts within the framework of the current legislation and with the exclusive purpose of receiving preventive information in case there is threat of a cybercrime or in the course of conduction of investigative and technical search in telecom systems or channels which may be used by cyber criminals;

provides through the **structural department for combatting cybercrime** of the Ministry of Internal Affairs for the coordination of the activities of the subjects of combatting cybercrime in

accordance with the competence established by the legislation of Ukraine; carries out pre-trial investigation in cases connected with the use of computer technologies;

initiates the arrest for an indefinite period of time of the assets, connected with the financing of crimes which use computer technologies and refer to financial operations suspended in accordance with the UN Security Council decisions, the relieve of these assets from arrest and provision of access to them upon the application of a person, who may provide documental evidence of the need to cover fundamental or extraordinary expenditures;

provides in coordination with the Security Service of Ukraine for the protection from criminal encroachments using computer technologies of Ukrainian establishments, including those located outside its territory, their employees and their families.

The Security Service of Ukraine combats cybercrime through prevention, discovery and termination of crimes committed using computer technologies, the investigation of which in accordance with Ukrainian law falls under the competence of the departments of the Security Service of Ukraine.

The Ministry of Defense combats cyber threats via prevention, discovery and termination of threats to the defense of the state which are carried out with the help of computer technologies.

The central executive authorities which provide for the formation and implementation of state policy in the field of civil protection, as well as administrative bodies subordinated to them, in cases connected with the use of computer technologies participate in activities to minimize and eliminate the consequences of these situations while conducting operations to counter crimes related to the use of computer technologies, and also implement public education and outreach activities to prepare the population for safe work in the field of computer technologies.

Article 8. Authority of other subjects involved in combatting cybercrime

The subjects which are involved in combatting cybercrime within their competence carry out measures to prevent, discover

and terminate crimes connected with the use of computer technologies; develop and implement preventive, routine, organizational, educational and other activities; provide conditions for conducting operations to counter cybercrime at facilities which fall under their field of administration; provide the respective departments for the time of such operations with hardware and financing, transportation and communication means, other tools, as well as information required to perform tasks regarding combatting cybercrime.

Article 9. Interaction of the subjects in the field of preventing and combatting crime in the field of computer information

Under the framework of preventing and countering crime in the field of computer information the competent authorities, service providers, NGOs and other civil society agents shall cooperate via exchange of information, experts, conduction of joint activities for the solution of crimes and discovery of perpetrators, staff training, implementation of initiatives in order to conduct programs, practices, activities, procedures, implementation of minimal standards for the security of computer systems, implementation of educational campaigns aimed at informing of computer crime and the risks which the users of computer systems run, as well as carry out other activities in this field.

Article 10. Provision of support to the bodies which combat cybercrime

The state bodies, local self-government, unions of citizens, organizations and their officials shall support the bodies which combat cybercrime, notify of the data which they have become aware of regarding computer crimes, or any other circumstances in this regard the information on which may promote the prevention, discovery and termination of crime connected with computer technologies, or the minimization of its consequences.

Article 11. Obligations of the owners of computer systems

The owners of computer systems, access to which is prohibited or restricted for certain types of users, must inform the users about

the legal conditions for access to these computer systems. This warning must be accessible for every user.

Article 12. Obligations of the service provider

The service providers must:

a) keep records of the users of the services;

b) inform the competent bodies about information flows, including illegal access to information from computer systems, attempts to introduce illegal software, violation by the responsible persons of the rules for collection, processing, storage, dissemination and division of information or the rules for protection of a computer system established based on the status of data or its protection level, in the case these actions supported appropriation, alteration or destruction of data, or caused other grave consequences, such as disruption of functioning of computer systems or other computer violations;

c) respond in confidential mode in accordance with the current law to the requests of competent bodies about the immediate saving of computer data or data on information flows with regard to which there is a threat of its destruction or damage, for a term of no more than 90 calendar days;

d) provide the competent authorities with information in answer to requests, submitted under the law, namely – data on the users, including the appearance of the notification from the service used by the user, and the way of payment for this service;

e) take security measures by applying certain procedures, devices or specialized computer software with the help of which access to the computer system is restricted or prohibited for unauthorized users;

f) provide for monitoring, surveillance and preservation of data flows for the identification of the providers of services, their users and the channel by which the message was transmitted, for a term of 360 calendar days;

g) provide for the decryption of computer data contained in the network protocol packets, and store this data for 120 calendar days.

In the case when the data on information flows is owned by several service providers, the service provider who received the request must immediately provide the competent body with the information required to identify the other service providers.

Chapter III

ELIMINATION OF THE CONSEQUENCES OF CYBERCRIME AND OTHER VIOLATIONS OF THE LAW CONNECTED TO CYBERCRIME

Article 13. Restriction of access to information which is provided with violations of the current law

In the case of discovery on information and telecommunications networks, including the Internet, of information which is provided with violations of the current law, contains appeals to mass riots, conduction of extremist activities, participation in mass (public) activities conducted with violations of the established order, including instances of provision of this information by the state and local authorities, organizations or citizens, **as well as in the cases of use of networks and (or) communication means with criminal goals, which harm the interests of a person, the society and the state, and the dissemination of information which violates the legislation on elections in Ukraine, the Prosecutor General of Ukraine or his/her deputies shall apply to the authorized institution with a prescript to eliminate the violations of the law and suspend the work of the network and (or) communication means, the provision of communications services, access to internet resources and (or) information located thereon.**

In Ukraine this authorized body is the ***National Commission for Protection of Information and Information Technologies.***

The National Commission for Protection of Information and Information Technologies **is a collegial body of the state, subordinated to the President of Ukraine and reporting to the Verkhovna Rada of Ukraine. It is formed based on this Law by the President of Ukraine from among the managing staff of the Ministry of Internal Affairs, the Security Service of Ukraine, the Ministry of Defense, the National Commission for State Regulation in the Field of Communications and Informatization,**

representatives of the media and the public (upon their consent). The working apparatus of the Authorized body is a separate unit of the ***structural department for combatting cybercrime of the Ministry of Internal Affairs*****, established via using additional staffers.**

The Authorized body, based on the prescript mentioned in Paragraph 2 of this Law shall in the course of three hours after receiving the prescript shall:

1 – send to the communications operators through the interaction system a request to take measures to limit access to the information resource, including to Internet-sites or information located thereon, which contains information provided in violation of the current law, appeals to mass riots, conduction of extremist activities, participation in mass (public) activities conducted with violations of the established order, including instances of provision of this information by the state and local authorities, organizations or citizens, **as well as in the cases of use of networks and (or) communication means with criminal goals, which harm the interests of a person, the society and the state, and the dissemination of information which violates the legislation on elections in Ukraine**. This request shall contain the domain name of the site on the Internet, the network address, the data on web-site pages on the Internet, which allow identifying this information;

2 – establish the hosting provider or any other person who provides for the placement on the information and telecommunication network, including the Internet, of the aforementioned information resource, the servicing owner of the Internet-site which contains information provided in violation of the current law, appeals to mass riots, conduction of extremist activities, participation in mass (public) activities conducted with violations of the established order, including instances of provision of this information by the state and local authorities, organizations or citizens, **as well as in the cases of use of networks and (or) communication means with criminal goals, which harm the interests of a person, the society and the state, and the dissemination of information which violates the legislation on elections in Ukraine**;

3 – send to the hosting provider or another person indicated in

p. 2 of this paragraph an electronic message in English and Ukrainian about the violation of the procedure for dissemination of information, containing the domain name and network address which allow identifying on the Internet the web-site which contains information provided in violation of the current law, appeals to mass riots, conduction of extremist activities, participation in mass (public) activities conducted with violations of the established order, including instances of provision of this information by the state and local authorities, organizations or citizens, **as well as in the cases of use of networks and (or) communication means with criminal goals, which harm the interests of a person, the society and the state, and the dissemination of information which violates the legislation on elections in Ukraine**, as well as data on the pages of the Internet-site which allows identifying this information, together with a request to take action to delete this data;

4 – record the date and time of sending the request to the hosting provider or any other person indicated in p. 2 of this paragraph with a request to eliminate the violations of the procedure for disseminating information.

After receiving via the interaction network the request from the **National Commission for Protection of Information and Information Technologies** about talking action to restrict access, the communications operator which provides services regarding access to the information and telecommunication network "Internet" must immediately, in no more than one hour from the moment of receiving the request of the Authorized body, restrict access to the information resource, including access to an Internet-site, or to information placed thereon, which contains information provided in violation of the current law, appeals to mass riots, conduction of extremist activities, participation in mass (public) activities conducted with violations of the established order, including instances of provision of this information by the state and local authorities, organizations or citizens, **as well as in the cases of use of networks and (or) communication means with criminal goals, which harm the interests of a person, the society and the state, and the dissemination of information which violates the legislation on elections in Ukraine**.

During **no more than three hours** after receiving the

notification mentioned in p. 1 of paragraph 3 of this Article, the hosting provider or any other person mentioned in p.2 of paragraph 3 of this Article shall inform thereof the servicing owner and request the immediate removal of information provided in violation of the current law, appeals to mass riots, conduction of extremist activities, participation in mass (public) activities conducted with violations of the established order, including instances of provision of this information by the state and local authorities, organizations or citizens, **as well as in the cases of use of networks and (or) communication means with criminal goals, which harm the interests of a person, the society and the state, and the dissemination of information which violates the legislation on elections in Ukraine**.

In the case the owner of the information resource deleted information containing appeals to mass riots, conduction of extremist activities, participation in mass (public) activities conducted with violations of the established order, including instances of provision of this information by the state and local authorities, organizations or citizens, **as well as in the cases of use of networks and (or) communication means with criminal goals, which harm the interests of a person, the society and the state, and the dissemination of information which violates the legislation on elections in Ukraine,** he/she shall send official notification thereof to the ***National Commission for Protection of Information and Information Technologies***. This notification may be sent in electronic format and signed by electronic signature.

After receiving the notification mentioned in paragraph 6 of this Article and the verification of its authenticity, the ***National Commission for Protection of Information and Information Technologies*** must immediately inform via the interaction system the communications operator who provides services on access to the Internet about the restoration of access to the information resource, including Internet sites.

After receiving the notification mentioned in paragraph 7 of this Article, the communications operator shall immediately restore access to the information resource, including Internet-sites, and officially inform thereof the ***National Commission for Protection of Information and Information Technologies, the office of the General Prosecutor, and the Structural Department***

for Combatting Cybercrime of the Ministry of Internal Affairs.

Article 14. Compensation of damage

Damage, incurred upon the state, enterprise, institution, organization or natural person as a result of a cybercrime shall be compensated by the guilty persons based on general grounds and conditions of liability for damages.

In the case of refusal of the guilty person to return credit, loans, securities, immovable property or any other property illegally received using computer technologies, the property in question or its value shall be levied (confiscated) to the state revenue via court process upon the application of the prosecutor.

The receipt of subsidies, subventions, allowances, credits and benefits as a result of a cybercrime, shall render the concluded contract null and void with all the consequences provided for by the Civil Code of Ukraine (1540-06).

Article 15. Cancellation of illegal regulations and decisions passed as a result of a cybercrime

Illegal regulations and decisions passed as a result of a cybercrime shall be cancelled by the body or official authorized to take and cancel respective acts and decisions, or shall be recognized illegal in court.

Article 16. Restoration of rights and compensation of damage to natural persons and legal entities

Natural persons and legal entities the rights of which have been violated as a result of cybercrime and who have suffered moral or pecuniary damage are entitled to the restoration of their rights and compensation of damage in accordance with the process established by the law.

Chapter IV

INTERNATIONAL COOPERATION

Article 17. Main principles of international cooperation in the field of combatting cybercrime

Ukraine cooperates with other countries, their law enforcement and special services, as well as with international organizations which combat cybercrime following its international treaties, the law, and the obligations provided for by the international

agreements to which Ukraine is a party to.

This cooperation includes:

international assistance in the field of criminal law;

extradition;

identification;

blocking, sequestration and confiscation of products and instruments of the crime;

conduction of joint investigations;

information exchange;

training of staffers in this field of activity.

Article 18. Joint operational and investigative activities and criminal prosecution

Upon request of Ukraine's competent bodies or the competent bodies of other states, joint operations and investigations may be carried out on the territory of Ukraine aimed at preventing and combatting crime in the field of computer technologies in accordance with the law and under the framework of criminal prosecution.

Joint investigations may also be carried out based on bilateral and multilateral agreements concluded by competent bodies.

The representatives of competent Ukrainian bodies may participate in joint investigations carried out on the territory of other states, with the observation of the legislation of these states.

Article 19. Provision of information upon requests of competent bodies of other states

Ukraine shall provide information on issues connected with combatting cybercrime to a foreign state based on an application, while observing the requirements of Ukrainian law and its international and legal obligations.

Under the framework of international cooperation the competent bodies of other states may request from the competent bodies of Ukraine the immediate storage of computer data or

information flow data existing on any computer network on the territory of Ukraine, with regard to which the competent body of the other state must prepare a well-grounded request for the provision of international legal assistance in the field of criminal law.

The request to immediately store computer data must contain:

- the name of the body which makes the request;

- a brief explanation of the facts which are the object of criminal prosecution, their legal justification;

- computer data, the storage of which is being requested;

- any available information to identify the owner of computer data and discover the computer system;

- the valuableness of computer data and the need to save it;

- the intentions of the competent bodies of other states need to be formulated as a request to provide international legal assistance in the field of criminal law.

The term of preservation of the data mentioned in paragraph 1 of this Article may not be less than 60 calendar days and remains valid until the passage by a competent body of Ukraine of the decision about providing international legal assistance in the field of criminal law.

The transfer of computer data is carried out only after the acceptance by a competent body of Ukraine of a request on the provision of international legal assistance in the field of criminal law.

Article 20. Confidentiality and restrictions of using computer data

In case there are no active agreements on mutual support or treaties based on the same or mutual legislation between the requesting Party and the Party which receives the request, the provisions of this Article shall apply.

The provisions of this Article shall not apply in the case there is such an agreement, treaty or legislation, unless the interested parties agree to apply instead the provisions of this Article below, in part or in full.

The Party, which receives the request, may establish as a requisite for the provision of information that this information is kept confidential, and that the request about mutual legal assistance will not be satisfied in case of the absence of this condition, and the data will not be used for investigation or prosecution purposes other than those mentioned in the request.

In the case the Party which requests the information is unable to comply with the condition established by paragraph 2 of this Article, it shall immediately inform thereof the other Party, which will later decide, whether the information could be provided in spite of this.

In case the requesting Party accepts this condition, it becomes binding for it.

Any Party providing information or materials based on the condition established in paragraph 2 of this Article may require the other Party to provide an explanation on using this information in connection with this condition.

Article 21. Extradition of persons who participated in cybercrimes

The commission of a crime by foreigners or stateless persons which are not permanent residents of Ukraine may serve as grounds to extradite these persons to another state for bringing them to criminal responsibility.

The extradition of persons mentioned in part 1 of this Article with the goal of their criminal prosecution and the execution of binding acts of a foreign state shall be conducted in accordance with the law and the obligations assumed by Ukraine as a result of the ratification of the European Convention on Extradition (995_033), 1957, the European Convention on Cybercrime (994_789), 2001, and other international agreements the consent to the binding nature of which has been given by the Verkhovna Rada of Ukraine, as well as on a reciprocal basis.

Chapter V

RESPONSIBILITY

Article 22. Responsibility for the violation of this law

The violation of this law entails disciplinary, civil, administrative or criminal responsibility under the legislation of Ukraine.

Chapter VI

CONTROL AND SUPERVISION OVER THE LEGALITY OF COMBATTING CYBERCRIME

Article 23. Control over combatting cybercrime

Control over the observation of the law while combatting cybercrime is carried out by the Verkhovna Rada of Ukraine in accordance with the procedure established by the Constitution of Ukraine. Control over the activities of the subjects of combatting cybercrime is carried out by the President of Ukraine and the Cabinet of Ministers of Ukraine in accordance with the procedure, established by the Constitution and laws of Ukraine.

Chapter VII

TRANSITIONAL PROVISIONS

1. This Law shall take effect from the day of its official publication.

2. The Cabinet of Ministers of Ukraine in the course of three months after the taking effect of this Law shall:

bring its rules and regulations in conformity with this Law;

provide for the revision and cancellation by ministries and other central executive authorities of their rules and regulations which contradict this Law.