Preparatory Colloquium
Verona (Italy), *28 – 30 November 2012*
Section I - Information Society and Penal Law

Hungary*

András CSÚRI*

(A) Introduction and systematization

General Overview

Hungary signed the Council of Europe Convention on Cybercrime (hereinafter Convention)[1] in 2001. It was ratified by the Hungarian Parliament in 2003 and entered into force in July 2004. The Council of Europe stated in its most recent assessment of the countries cybercrime legislation (2007) that the Convention was implemented on a high level.[2]

The relevant rules are located primarily in the Criminal Code (CC)[3], in the Criminal Procedure Code (CPC)[4], in the Act on Electronic Commercial Services and on Certain Legal Aspects of Information Society Services[5] and in the Act on Electronic Communications[6]. Additionally, as criminal sanctions are generally considered to be of last resort[7], the legislative supports alternatives to criminalization, like self-regulations and code of ethics elaborated by the actors concerned.[8]

The countries laws were continually amended since the transition to democracy (in 1989-1990). Additional significant changes occurred since 2010 with the entering into force of a new constitution (January 2012)[9] and criminal code (July 2013). The latter amended the then existing cybercrime provisions and introduced new ones as well. In the light of the topicality (but lack of application) of the new provisions the analysis assesses both the rules of the 1978 and of

---

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

* Dr. András Csúri, Ph.D. is senior researcher at the Max Planck Institute for Foreign and International Criminal Law in Freiburg, Germany.

1 Convention on Cybercrime. ETS No. 185. See http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=185&CL=ENG for a link to the Convention including the database and signatures and ratifications.

2 http://www.coe.int/t/dg1/legalcooperation/economiccrime/cybercrime/documents/countryprofiles/567-LEG-country%20profile%20Hungary%20_7%20June%2007_En.pdf.

3 Act No C. of 2012. (2012. évi C. törvény a Büntető Törvénykönyvről).

4 Act No XIX. Of 1998. (1998. évi XIX. törvény a büntetőeljárásról).

5 Act 108/2001 on Electronic Commercial Services and on Certain Legal Aspects of Information Society Services. (2001. évi CVIII. törvény az elektronikus kereskedelmi szolgáltatások, valamint az információs társadalommal összefüggő szolgáltatások egyes kérdéseiről).

6 Act C. of 2003 on Electronic Communications. (2003. évi C. törvény az elektronikus hírközlésről.)

7 This is supported by several decisions of the Constitutional Court. See decisions 30/1992. (V.26.) or 18/2000. (VI.6.).

8 See below E.

9 Magyarország Alaptörvénye (2011. április 25.).

the 2012 criminal codes. The sources from the Criminal Code of 1978[10] are indicated as fCC, while references to the new code are made as CC.

Systematization of the relevant crimes

This study differentiates between two groups of cybercrimes. *Cybercrimes in the strict sense* are made up of offences, which are committed solely within or by means of a computer/information system. The relevant provisions protect primarily the integrity of information systems and data (group one). *Cybercrimes in the broad sense* consist of offences that are either not necessarily committed by means of computer systems or protect legal interests not exclusively related to cybercrimes (group two). Typical examples for the second group are copyright infringements, child pornography, crimes related to the integrity of privacy, computer-related forgery and computer-related fraud.[11]

The Criminal Code of 1978

The Criminal Code of 1978 remained in force until 1 July 2013. It did not contain a separate chapter on cybercrimes. The chapter on economic crimes comprised *cybercrimes in the strict sense* in the form of the offences of "Crime against the integrity of computer systems and data" (Art. 300/C fCC) and the "Deception of the Computer System Security" (Art. 300/E fCC). *Cybercrimes in the broad sense* were spread in most different chapters of the criminal code. They took shape amongst others in offences related to copyright infringements (Art. 329/A and 329/B fCC) and to the integrity of privacy, such as "Stalking" (Art. 176/A fCC), "Abuse of Personal Data" (Art. 177/A fCC) and "Obtaining Private Secrets" (Art.178/A d) fCC). Additionally, in the sexual-related crime of "Abuse of Illicit Pornographic material" (Art. 204 fCC).[12]The chapter on economic crimes also contained some cybercrimes of the second group, such as "Computer-related forgery" (Art. 300/C fCC), "Computer-related fraud" (Art. 300/C fCC), "Non-cash payment forgery" (Art. 313/B fCC) and "Non-cash payment fraud" (Art. 313/C fCC).

The Criminal Code of 2012

The new code introduced changes in the terminology, structuring and sanctioning of cybercrimes. In general, the *term* "computer" was replaced by "information systems and data", while the more specific phrase of "child pornography" took the place of "illicit pornography".

Regarding the *structuring* of cybercrimes, a separate chapter on "Illicit Data Gathering and Crimes against Information Systems" was established. The new chapter covers cybercrimes in the strict sense. These are "Illicit Data Gathering" (Art. 422 sub. 1 d) CC), "Crimes against the Integrity of Information Systems and Data" (Art. 423 CC) and "Deception of the Information System Security" (Art. 424 CC). "Illicit Data Gathering" is the amended form of "Obtaining Private Secrets", which was previously defined as a crime against personal freedoms and dignity (Art. 178 fCC). Cybercrimes in the broad sense are still spread in different chapters of the code. These are most importantly crimes related to copyright infringements" (Art. 384 and 386. CC) and to the integrity of privacy ("Stalking" Art. 222 CC; "Abuse of Personal Data" (Art. 219 CC)). Additionally, sexual related crimes like "Child Pornography" (Art. 204 CC) and property crimes, such as "Information system related forgery" (Art. 375 CC); "Information system related fraud" (Art. 375 CC); "Non-cash payment forgery" (Art. 393 CC) and "Non-cash payment fraud" (Art. 392 CC).[13]

---

[10] Act IV of 1978 (1978. évi IV. Törvény a Büntető Törvénykönyvről).

[11] The report focuses primarily on cybercrimes in the strict sense. Cybercrimes in the broad sense are only dealt with when necessary with regard to the questionnaire.

[12] See also Z A Nagy, *Bűncselekmények számítógépes környezetben*, (Budapest, ad librum, 2009)

[13] Accordingly, information system related fraud and forgery are now classified primarily as crimes against property.

Finally, the new code introduced a cybercrime-related *sanction* (applicable even if the perpetrator is not criminally liable), which obliges providers to make certain data inaccessible in a final manner (Art.77. CC).

(B) Criminalization

(1) Which specific legal interests are deemed to be in need of protection by criminal law?

In the Criminal Code of 1978, cybercrimes in the strict sense protected the legal interests to the *integrity and proper functioning of information systems and the integrity of data.* Nevertheless, these offences were classified as economic crimes and so protected economic interests in the first place. The new code moved these offences to the chapter on"Illicit data gathering and Crimes against Information Systems", which emphasizes that these protect legal interests connected to cyber law in the first place.

(2) Typical examples concerning:

(a) attacks against IT systems

In accordance with Art. 2 of the Convention, the new criminal code continues to criminalize the illegal *access* to information systems. Additionally, it also criminalizes if someone *stays* in an information system (following legal access) outside his/her authority (Art. 423 sub 1. a) CC).

(b) violation of IT privacy

The new code continues to protect *IT privacy* on a rather low level. The accompanying practice will be presented with the example of the webpage "pedomaci.hu"[14], which recycled images of minors paired with sexual innuendoes ("pedomaci-case"). The original images were downloaded from websites and social networks and intended to generate revenues from the advertisements on the website. The webpage was not banned, as the public prosecutor's office ruled that the owners of the images *assigned their right to protection* by publishing the pictures on public web pages.[15]

Privacy in the traditional sense continues to be protected by the current criminal code. Most notably by the provisions of "Obtaining Private Secrets" (178/A d fCC and Art. 422 d) CC) and the "Abuse of Personal Data" (Art 177/A fCC and Art. 219 CC), which may be committed by means of computers as well. The new code moved "Obtaining Private Secrets" to cybercrimes and changed (and so broadened) the object acted upon from "private secrets" to "data". Thus, the new provision protects the legal interest to IT privacy in the first place.

(c) forgery and manipulation of digitally stored data

The Criminal Code of 1978 protected the *integrity of data* subsidiary to other legal interests, such as the proper functioning of the computer system or economic interests. A good example provides the former offence of "Integrity of computer systems", whereby the misuse of data was subsidiary to obtaining illicit benefits (Art. 300/C. (3) a) fCC).

---

[14] The name is a combination of the Greek words of child or slave (pais or in English spelling paedo) and the Hungarian word of little bear (maci). "Pedo" being also a short form and "pedobear" an internet meme for paedophiles. This all together suggest the addressees of the site.

[15] Despite the ruling, the websites domain name was removed as it referred to the sexual exploitation of minors. Further, the host provider (an anonymiser service) removed the offensive contents. See K Parti, L Marin, *'Ensuring freedoms and protecting rights in the governance of the internet: A comparative analysis on blocking measures and internet providers' removal of illegal internet content'*, in jcer.net Vol. 9. Issue 1. 2013 150.

The newly amended provision provides for a stronger protection by no longer connecting the protection of the integrity of data to other legal interests. (Art. 423 sub. 1 c) fCC).

(d) distribution of computer viruses

A court decision assessed the distribution of computer viruses as a criminal attempt against the integrity of the computer system.[16] Nevertheless, there is no specific provision on the distribution of computer viruses in the criminal code.

(e) crimes related to virtual identities of users

No specific provisions exist in the criminal code regarding the virtual identities of users.

(f) other innovative criminal prohibitions

The Criminal Code of 2012 criminalizes the gathering of any kind of information related to *undercover agents* or people cooperating with the secret services. This more interesting than innovative new rule is regulated as a special form of "Illicit Data Gathering" (Art. 422 sub. 2 CC) and also serves as an example of bringing forward criminal liability.

(3) Actus reus and Definitions

How are criminal conduct/object typically defined?

The *criminal conduct* is defined either by the description of the act (e.g. "illegal access into the system"; Art. 423 sub. 1 a) CC)) or by the description along with the results of the act ("hindering the integrity of the system through the illegal modification of data"; Art. 423 sub.1 b) CC)).

The *objects* of these crimes (such as system or data) are defined in accordance with the definitions of the Convention. The Criminal Code of 1978 defined solely the meaning of "computer system". The new code replaced the term "computer system" by "information system". Further, it gives definition of "data" and "password", albeit solely with respect to specific offences (Art. 423 sub 4 CC; Art. 424 sub 3 CC). The Act on Electronic Commercial Services and on Certain Legal Aspects of Information Society Services defines "service providers", while the Act on Freedom of Information[17] defines several aspects of "personal data". The recently passed Act on Electronic Data Security of governmental and local institutions (Act on Electronic Data Security)[18] provides a list of 48 definitions regarding cyber law and so gives statutory basis for the current and future legal terminology (Art 1).

(4) Is criminal liability for certain cybercrime limited to particular groups of perpetrators and/or victims?

There are no personal qualifications required by law with regard to cybercrimes. Thus, both natural persons and legal entities can be perpetrators or victims of cybercrimes. As an exception, the "Abuse of Personal Data" can only be committed by persons entitled to work with such data. Further, an aggravated form of this offence can only be committed by *officials* (Art. 219 sub. 4 CC).

---

16 Court decision BH1999. 145.

17 Act CXX of 2011. (2011. évi CXX. Törvény az információs önrendelkezési jogról és az információszabadságról.).

18 Act L of 2013 on Electronic Data Security (2013. évi L törvény az állami és önkormányzati szervek elektronikus információbiztonságáról).

(5) Mens Rea

Does criminal liability in the area of ICT and internet extend to merely reckless or negligent conduct?

All cybercrimes in the criminal code are offences of intent. In several cases like the "Deception of the Information System Security" (Art. 424 sub. 1 CC) or "Illicit Data Gathering" (Art. 422 sub. 1 CC) the law even requires for direct intent (*dolus directus,* Art. 7 CC), thus the aim at a particular consequence of the act.

(6) Specific differences between the definitions of "traditional" crimes and cybercrimes

Are there specific differences between the definition of cyber crimes and "traditional" crimes?

The definitions of cybercrimes do not differ from those of "traditional" crimes. Nevertheless, in light of the quickening pace of technological change these offences focus more on the acts and their consequences and less on detailed modes and forms of perpetration.

(C) Legislative technique

(1) Principle of legality

No specific cybercrime-related problems occurred as yet with respect to the principle of legality.[19]

(2) Avoiding undue chilling effects on legitimate use of ICT and internet

The legislative support of alternatives to criminalization – like self-regulations and code of ethics – is one way to set frames to the legitimate use of internet (Art. 15/A of the Act on Electronic Commercial Services and on Certain Legal Aspects of Information Society Services). The strong requirement for intention in the definitions of cybercrimes (in many cases even direct intent) also serves to avoid undue chilling effects on legitimate use of the internet (see B. 5).

Finally, the new code introduced an excuse for peer-to-peer network architectures. According to this, the person is excused if the file was shared automatically while downloading it for personal use (Art. 385 CC). According to the explanatory notes of the law this excuse was introduced especially with respect to the user habits of young offenders.

(3) Rapid technological innovation

The explanatory notes of the new criminal code highlight with regard to cybercrimes that the legislator is always behind the quickening pace of *technological change*.[20] Accordingly, new provisions, like the "Integrity of Information Systems and Data" (Art. 423 HCC), focus rather on the act and its results than on the forms of its perpetration.

The cybercrime-related provisions of the Hungarian criminal codes focused constantly more on the integrity of the information system and data and less on the virtual identity, habits or privacy of the users (see "pedomaci-case"; B.2.b.). However, some few studies (for example within the frame of the World Internet Project)[21] as well as the central statistics[22] do offer some insights on user habits. According to these, despite upward trends there is still

---

[19] T Hüttl, E Jovánovics, M D Szabó, B Vissy, *'Alkotmánybíróságok az adatmegőrzésről. Adalékok az Alkotmánybíróság számára az adatmegőrzési irányelvet átültető Magyar szabályok alkotmányossági felülvizsgálatáról szóló eljárásához'* in Infokommunikáció és Jog 2010/2, 69-73.

[20] Similarly, the explanatory notes to Art. 159/A of the Act on Electronic Communications. See also L Köhalmi, *'A gazdasági és a szervezett bűnözés'* in E Csemáné Váradi (ed.) Bevezetés a bűnügyi tudományokba, (Miskolc, Bíbor, 2007). 147.

[21] http://www.worldinternetproject.net/#about

[22] See for example the 2011 statistics regarding the use of internet. Hungarian Central Statistical Office. http://www.ksh.hu/docs/hun/xftp/gyor/tav/tav21109.pdf

infrequent access to internet in the Hungarian households. Further, there is a general distrust towards online business transactions with the possibility of online banking remaining almost unused.[23] The user habits of children were specifically assessed as well.[24] The results of such studies should be taken into account, when drafting future laws. As mentioned above the new code did introduce an excuse especially with respect to peer-to-peer network architectures and the user habits of young internet users. According to this a person is not punishable if the download automatically shares the file with others (Art. 385 CC; See C.2.).

(D) Extent of criminalization

(1) Preparatory acts

The preparation of crime involves first observable acts in order to complete a targeted crime. In Hungarian criminal law preparation constitutes criminal liability only if explicitly laid down in the criminal code (Art. 11. HCC). The offense of "Deception of the Information System Security" is comprised of such preparatory acts, like the purchase of data or making specific programs available (Art. 424 CC). It is therefore an "inchoate offense", which is nevertheless punished by law like a completed crime (*delictum sui generis)*. This however, is no exception in the criminal code. Similarly, the above mentioned criminalization of obtaining information about intelligence agents may serve as an example of criminalization of preparatory acts (Art. 422 sub.2 CC).

(2) The criminalization of mere possession of data

Both the former and the current forms of "Deception of the Information System Security" forbid the *acquisition* of passwords or programs in order to commit other crimes. The explanatory notes of the new code define acquisition – with regard to crimes against the privacy of communication – as the "illicit transfer of possession". The commentary takes notice of the fact, that Art. 6 of the Convention distinguish between the purchase and the possession of data. It emphasizes however, that in the Hungarian criminal law, the concept of acquisition (of data or programs) always comprises possession as well. Accordingly, the legislator did not see the need for a separate definition. The explanatory note further underlines, that while drafting the new code, the Draft Directive on Attacks against information systems[25] was taken into account as well, which does not apply the term "possession" any longer. On the grounds of the above mentioned argumentations, the Criminal Code of 2012 does penalize the mere possession of data without calling it by name.

(3) The criminal liability of providers

Internet Service Providers (ISP) have no general monitoring obligations concerning the contents they make available. Regarding notice and takedown of illegal contents the current law differentiates between ISPs. Solely commercial ISPs are obliged to notice and takedown illegal contents in relation to copyright infringements. Thus only commercial

---

[23] World Internet Project International Report. The Internet in Hungary. (Third edition, 2009). http://www.tarki.hu/hu/research/wip/index.html.

[24] K Parti,,Gy Virág, *'Valós kockázatok és lehetőségek a virtuális kommunikációban. A kelet-európai gyerekek nethasználatának specifikumai*', http://kriminologia.hu/sites/default/files/2010eavszpartik_viraggy.pdf, 2012. K Parti,Gy Virág, *'Sweet child in time. Online sexual abuse of children – a research exploration*' in The Open Criminology Journal. Bentham Science Publishers URL: http://www.benthamscience.com/open/tocrij

[25] COM (2010) 517 Proposal for a Directive of the European Parliament and of the Council on attacks against information systems and repealing Council Framework Decision 2005/222/JHA. See also the proposal of the European Parliament: http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P7-TA-2013-0321+0+DOC+XML+V0//EN.

ISPs hold a limited liability (Act on Electronic Commercial Services and on Certain Legal Aspects of Information Society Services; Art. 13). Non-commercial ISPs may be challenged in civil disputes (See below E).

The *criminal law* regulations apply for all internet providers. The new criminal code introduced a *special sanction*, applicable even if the perpetrator is not criminally liable. This obliges providers at their own cost, to make *data inaccessible in a final manner* if it represents, results from or was the instrument of crime (Art. 77. CC). In July 2013 the possibility to make data *temporary inaccessible* was introduced into the Criminal Procedure Code. The measure is applicable if it prevents from further crimes and the concrete offence is punishable by making data inaccessible in a final manner (Art. 158/B CPC). The order is given by a judge and the data must be made inaccessible within one working day (Art 158/C sub 1 CPC). Providers failing to fill their duty can be fined repeatedly (Art 158/C sub 1 and 6 CPC).

(4) Criminal sanctions targeting cyber criminals

The new criminal code introduced a cybercrime-related sanction. This allows for *making content data inaccessible* in a final manner if it represents, results from or was the instrument of crime (Art. 77. CC). It is applicable even if the perpetrator can not be hold criminally liable. As the sanction was introduced most recently, no evaluation of the practice can be presented. The explanatory notes emphasis that the new sanction was introduced in connection with Art. 25 of the 2011/92 EU directive regarding child pornography,[26] which demands from Member States to ensure the removal of web pages containing or disseminating child pornography.[27] There are no specific sanctions in relation to the *perpetrators* of cybercrimes (like a temporary ban on using the internet in general).

(E) Alternatives to Criminalization

The legal base of alternatives to criminalization is provided for in the Act on Electronic Commercial Services and on Certain Legal Aspects of Information Society Services. According to this, the state supports the elaboration of self-regulations and code of ethics by the relevant actors (Art. 15/A). The Act also encourages alternative dispute resolutions. This approach is supported by several decisions of the Constitutional Court, which see criminal sanctions as a last resort.[28]

The Association of Hungarian Content Providers[29] elaborated such a code of ethics. It contains operational, ethical and procedural rules and provides sanctions against members who violate these rules. The sanctions range from the removal of content or the temporary ban from practicing member rights to the withdrawal of membership (Art. 13.). Additionally, the Hungarian Association of Content Industry defines as one of its basic tasks to "watch over the professional and ethical norms of the IT-sector and to take steps against practices violating generally accepted norms."[30]

Complaints may be addressed directly to specific online services. By way of example, the website "Biztonságos Internet" (Secure Internet) was established in April 2011 and serves as a hotline to report illegal and harmful contents

[26] Directive 2011/92/EU of the European Parliament and of the Council of Europe of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JHA.
[27] http://www.kormany.hu/download/9/32/b0000/IBTV_2012_10_12.pdf#!DocumentBrowse.
[28] Constitutional Court Decisions 30/1992. (V.26.) and 18/2000. (VI.6.).
[29] Magyarországi Tartalomszolgáltatók Egyseülete.
[30] http://www.matisz.hu/?id=257.

under the ".hu" ccTLD domain. The site operates according to the INHOPE standards[31] and aims to protect minors from the threats of internet.[32]

As of June 2013, the governmental CSIRT tasks were carried out by a public association named the National Cyber-security Center. It coordinated responses to serious IT security breaches against government networks and critical information infrastructures on a 24/7 service basis.[33] The recently passed Act on Electronic Data Security transferred these tasks to a future CSIRT at a central, governmental level (Art. 19 and 20).

The example of the trade related aspects of intellectual property rights also demonstrates the various alternatives to criminalization. Intellectual property rights are under the general protection of the Constitution (Art X.). Further there is a specific Act on Intellectual property rights[34]. If the copyright infringements are related to personal rights, civil law may also play a decisive role for the compensation of damages and lost profits.[35] Finally, criminal sanctions – as last resort – may be imposed if the infringement resulted in damages above a certain threshold (Art. 385 CC)

(F) Limitation of anonymity

Are there laws or regulations obliging internet service providers to store users' personal data, including history of internet use? Can providers be obliged to provide such data to law enforcement agencies?

The Act on Electronic Communication – in accordance with the Directive on privacy and electronic communications[36] – *generally* obliges internet service providers to retain user related data for purposes of criminal investigations, national security and national defence for a limited period of twelve months (Art. 159/A sub 3).[37] The Criminal Procedure Code obliges providers to retain data unaltered and possibly separate for *concrete* investigations. Providers must prevent any unauthorised changes to the data for a maximum period of three months (Art. 158/A sub 3. and 8 CPC). Thus the providers' rights are restricted regarding the relevant data for this limited period.

(G) Internationalisation

Hungary was deeply involved in the development of the Council of Europe Convention on Cybercrime which in fact was signed in Budapest. Within a year after signing the Convention the Criminal Code of 1978 was amended. According to the assessment of the Council of Europe, the Convention was implemented into national law on a high level.[38]

The country continues to participate in further discussions regarding the harmonisation of cybercrime legislation, amongst other things, as member of the open-ended intergovernmental expert group on cybercrime.[39]

---

31 http://www.inhope.org/gns/about-us/about-inhope.aspx
32 http://www.biztonsagosinternet.hu/en
33 http://www.cert-hungary.hu/en/node/69
34 Act No LXXVI. of 1999 on Intellectual Property Rights (1999. évi LXXVI. Törvény a szerzői jogról).
35 Act IV of 1959. The Civil Code of Hungary. (1959. évi IV. Törvény a Polgári Törvénykönyvről).
36 Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector. O.J. L 201, 31.7.2002, 37–47.
37 In case of ineffective calls for a period of six months (Art 159/A sub 3.).
38 http://www.coe.int/t/dg1/legalcooperation/economiccrime/cybercrime/documents/countryprofiles/567-LEG-country%20profile%20Hungary%20_7%20June%2007_En.pdf
39 http://www.unodc.org/documents/treaties/organized_crime/EGM_cybercrime_2011/UNODC_CCPCJ_EG4_2011_INF_2_Rev1.pdf

In accordance with the Convention (Art. 6 sub 1. a)), the new code introduced and criminalise the transmittal of passwords in case of "Deception of the Information System Security" (Art. 424 sub. 1 a CC).

The explanatory notes of the Criminal Code of 2012 refer to the Draft Directive on Attacks against Information Systems on several points.[40] Additionally, the terminology of the new code was adapted to the terminology of the Directive (see D 2).

Finally, the 2011 amendment of the Act on Electronic Communication extended its jurisdiction also to data posted on the Internet abroad (Art. 1. Sub 1.a)).

(H) Future developments

Current trends of legislation and legal debate concerning ICT and internet crime

As constantly indicated, the new Criminal Code entered into force recently, in July 2013. The report analysed the provisions of the new code and generally attempted to incorporate the most recent changes in the field of cyber law in Hungary. As with all new laws, these regulations aim to include the latest developments in their subject fields. On these grounds, there is not much space left for deliberations on desired developments of the near future.

Nevertheless, some provisions in the new laws highlight *future tasks*. The Act on Electronic Data Security requires the assessment and security-ranking of the information systems of government related institutions (Art. 7 and 8). Further, by providing a list of 48 definitions, the law gives statutory basis for the terminology of cyberspace related future legislation (Art 1). It also provides a legal base for a new CSIRT at a central, governmental level. The latter means that several powers exercised currently by a public association (see E) will be transferred to this "national CSIRT" in the near future (Art. 19 and 20).

The new criminal code established a *separate chapter* on cybercrimes in the strict sense (see above A.) and revised the structure of the offences. In light of the quickening pace of technological change it focuses rather on the acts and their consequences and less on the modes and forms of perpetration. The code introduced a special cybercrime-related sanction, which allows making crime-related contents permanently inaccessible. Assessing the application of these new provisions is for academics a future task in itself.

[40] European Parliament legislative resolution of 4 July 2013 on the proposal for a directive of the European Parliament and of the Council on attacks against information systems and repealing Council Framework Decision 2005/222/JHA (COM(2010)0517 – C7-0293/2010 – 2010/0273(COD)).