AARMS Vol. 14, No. 4 (2015) 281–289.

Information Security Law and Strategy in Hungary

SZÁDECZKY Tamás[1]

Information security has an emerging importance, even in people's daily life, even in country-level policymaking, but these two are inseparable. National information security strategy, applied legal regulation and the actual awareness of citizens are interconnected. The article shows the legal regulation of the last decades in Hungary, the relevant laws and their impact on information security, based on the legal aspects of cybersecurity and cyberterrorism. The focal points in the legislation are the Act on Electronic Public Service of 2009 and the Information Security Act of 2013. The paper points to the advancing interest on the cybersecurity by the side of the government and therefore the more and more detailed legal regulation implied by that.

Keywords: *information security act, cyber strategy*

Introduction

In the last seven decades there was a huge advance in information technology. From the time Konrad Zuse made the first Turing complete computer in 1941 and the building of Electronic Numerical Integrator and Computer (ENIAC), the first really universal computer in 1946, information security continuously has been a part of information technology. [1: 206] In the beginning it had a narrow joint focus, but it has been gradually widened.

We should notice that computers have been processing sensitive data from their early application, for example ENIAC was used to solve numerical problems regarding US military operations like the calculation of artillery firing tables. At that time physical security measures were enough to prevent unauthorized access. The general use of computers began with the implementation of multi-user mainframe computers from the 1950s mostly by IBM. Due to the fact, that multiple users were accessing those mainframe systems, access control measures had to be implemented. Universities were real playgrounds for hackers, who were testing the boundaries of those systems. Soon, interconnecting of standalone systems became a usual solution to increase efficiency and collaboration. The first point-to-point serial cable-based connections were inefficient, thus the Advanced Research Projects Agency (ARPA) started the "Intergalactic Network" initiative to use the existing telex network for computer communication in 1962. [2: 65] Later ARPA started the ARPANET network in 1969 which connected University of California, Los Angeles (UCLA), Stanford Research Institute's Augmentation Research Center, University of California, Santa Barbara (UCSB), University of Utah's Computer Science Department in the beginning, but later it was broadened and its name changed to Internet. Networking technologies have implied the development of a new branch of information security: network security.

1 Ph.D., National University of Public Service, Faculty of Public Administration, Department of Information Security; Hungary, Budapest; e-mail: szadeczky.tamas@uni-nke.hu

Network security had to deal with phenomena like eavesdropping and man-in-the-middle attacks, and at the same time the importance of cryptographic measures has become more important than in the case of the defense of a standalone computer.

Recently with the usage of portable computers, notebooks, mobile phones, smartphones and tablets and especially with bring your own device (BYOD) phenomenon the integration and secure connection to protected networks and security of data on the move have become new issues. Cloud computing technologies solved some problems of reliability and business continuity, while at the same time they also generated new issues in outsourcing security, data portability and segregation.

A whole virtual world or cyberspace has emerged on the basis of the technologies. No matter how strange but real world phenomena occur in this virtual world with more or less the same symptoms as in "off-line crimes". Criminologists and lawyers can debate that the perpetration of certain crimes in the virtual world and real world differ or not, but the method of protection and security technology is unanimously thought to differ from the real world, because you do not have to set up firewall rules or Access Control Lists (ACLs) in real life. Information security absorbs elements from the traditional security areas such as military defense, burglar alarm or fire prevention, but it also has new attributes.

New technologies appearing each year. Most of them cause new problems, open new vulnerabilities which should be solved by information security indicating a major professional problem. That is, information security solutions are always following controls by nature, because there is a natural delay between the implementation of the technology and the implementation of the effective and adequate security control. One of the main reasons for this is that at the time of development the developers found some security issues and implemented some security controls against them, but more problems and vulnerabilities are visible afterwards, when hackers challenge systems. At this point we have to implement newer and newer controls to protect systems. This is a never-ending story which needs continuous awareness on the part of security. According to recent empirical research, the information security awareness level in the Hungarian business sector needs further improvement. [3]

Intensive improvement of technology, high business demands and low time-to-market times do not urge application development industry to enhance security controls with the same speed as functional features, so security of network-based activities did not reach a reassuring level. Improvement and legal application of public key cryptography and strong secret key algorithms gave way to computer users for secure communications, but it is still not enough. Security of computer hardware elements, computer systems or networks depend on the full architecture, thus the weakest link determines the security level of the overall system.

In those early decades the security profession fought for the legitimacy of cyber security, and attention from high level management, which more or less knew the importance of this field. The question at the beginning of the twenty-first century is not the *why* but the *how* and *how much*. In the business sector, especially in times of economic crisis, cost constraint cannot be severe and we cannot imagine any compulsory expenditure from which managers do not want to cut off a bit. Management's objective is to devote usually minimal effort to IT security elements, systems and networks. Goals for citizens, shareholders, stakeholders and the government are the same: adequate information security level should be established and maintained. Every day we find that the decrease in IT budget implying much greater decreases in security budgets, and while in the case of a major telecom company it is hard to find

serious deficiencies, home computer users often do not install minimum preventions such as free security tools. Obviously this happens for many reasons: for example lack of technical knowledge, experience, information, money, or interest. But the most important thing is that most users do not draw enough attention to this area, despite the fact that later they might be liable for consequences.

The legislator's point of view, everything can be improved and the main goal is to reach a hundred percent perfection in the area. Therefore the field of information security also deals with this more general problem of security awareness.

The aim of this research was to analyze the change of the Hungarian legal regulation of information security in a chronologic manner in order to define categories of government strategies.

The Beginning

Technology development, as we described above, made local system security improvements indispensable. In case of e-government systems a higher level of problem also exists: attack against multiple systems or against a full infrastructure. This can be part of a conventional war, as cyberwar may be an unconventional event, and called cyberterrorist attack.

Cyberterrorism is a rather debated term and more scientific papers are analyzing this topic, so we should make an important note on the issue. According to Gorge [4: 9] the word cyberterrorism should be interpreted by its syllables, where cyberspace is the mass of computer communication networks. The term was created by William Gibson and was first used in the science fiction novel *Neuromancer*, which was written in 1984, describing a collective hallucination by billions of people. The term cyberspace emphasizes the close relationship between networks, relationships between people and networks, and social networks, in contrast to the earlier concept of network which has had primarily a technical meaning. According to Benjamin Netanyahu "Terrorism is the deliberate and systematic murder, maiming, and menacing of the innocent to inspire fear for political ends." [5: 20] According to the U.S. Federal Bureau of Investigation, cyberterrorism is any "premeditated, politically motivated attack against information, computer systems, computer programs, and data which results in violence against non-combatant targets by sub-national groups or clandestine agents." [6: 371]

But what kind of technical steps can a cyber-terrorist take?

On one hand the traditional way of using terrorism and information technology range from "soft" to propaganda methods. On the other hand they may apply "hard" methods, which are cyber warfare or hacking methods. [7] The same, or very similar, to what an "ordinary" online criminal does, and the differences are only in the impact and the effort. This is why we have to defend all individual systems in order to protect the entire infrastructure.

From the government's viewpoint generally we have to plan and prepare the national defense system against such actions. The first comprehensive security and defense policy system of Hungary after the political change in 1989 did not recognize cyber threats. Neither the National Assembly resolution no. 94/1998. (XII. 29.) on the security- and defense policy principles of the Republic of Hungary, nor the Government resolution no. 2073/2004. (IV. 15.) on the National Security Strategy of the Republic of Hungary, nor the Government res-

olution no. 1009/2009. (I. 30.) on the National Military Strategy of the Republic of Hungary included cyber defense as an objective. According to these policies and strategies defense against cyber-attacks are treated individually, even in the legal regulation.

We may find, however, an example of information security regulation in Hungary in the field of personal data protection (privacy or personally identifiable information protection in US law). [8]

As a general obligation all institutions managing and processing personal data, except private users have fallen under Act LXIII of 1992 on the Protection of Personal Data and the Disclosure of Information of Public Interest or later Act CXII of 2011 on informational self-determination and freedom of information. The security requirements were almost the same.

Section 7 (2) about data security requirements says that "data managers, and within their sphere of competence, data processors must implement adequate safeguards and appropriate technical and organizational measures to protect personal data, as well as adequate procedural rules to enforce the provisions of this Act and other regulations concerning confidentiality and security of data processing." [9] Relying on the analysis by András Jóri in his handbook [10] it can be claimed that data security and so a slice of informational security falls under the scope of the statutory regulation pertaining to data protection. According to subsection (3) "data must be protected by means of suitable measures against unauthorized access, alteration, transmission, public disclosure, deletion or destruction, as well as damage and accidental loss, and to ensure that stored data cannot be corrupted and rendered inaccessible due to any changes in or modification of the applied technique." [10: 258] The legislator gives examples of threats which in general correspond to standards. It is recommended to make a risk analysis about risks threatening the system and process of handling and processing data and about their occurrence. It is not required by the act on data protection, but normally it is required by all standards, so it is also a professional expectation.

This codification is not detailed, nor it is explanatory, and there are no controls built into it. Parliamentary Commissioner for Data Protection and Freedom of Information (later the Hungarian National Authority for Data Protection and Freedom of Information) supervised data management and data processing, but has no coercive measures; despite a part of data security being subject of personal data regulation. [10] The publicity is effective only in governmental cases.

Before the Act on Electronic Public Service (before 29 June 2009) there were no acts dealing with information security in public or governmental networks. [11: 4]

Only the following Government decrees regulated the field:

- 195/2005. (IX. 22.) Government Decree on security, interoperability and uniform use of electronic administration systems;
- 84/2007. (IV. 25.) Government Decree on security requirements of the Central Electronic Service System and related systems;
- 193/2005. (IX. 22.) Government Decree on Detailed rules for electronic filing;
- 194/2005. (IX. 22.) Government Decree on requirements for electronic signatures and the associated certificates used in the administrative proceedings, as well as requirements for certification service providers issuing the certificates;
- 182/2007. (VII. 10.) on the regulation of the central electronic service provider system.

These provided security rules sporadically to some systems, without any general framework. As a result we may say that relatively low awareness of the legislator and the business is observable in usage of international IT security standards, despite its significance and the high risk in some areas. No obligations found in acts of the Hungarian Parliament for enforcement of standards in IT security. There have been built-in self-control procedures in some acts, but in practice those procedures actually have not worked efficiently.

Transition

In 2009 a small change commenced with the adoption of Act LX of 2009 on electronic public services (abbreviated as Ekszt.). It has highlighted the requirement of security as a basic principle.

Organizations providing *Information and Communications Technology* (ICT) based public services ensure the publicity of data of public interest (according to the Act on data protection and freedom of information) and protection of personal and any other data during the provision of services. [12]

During the provision of services particular attention must be also be paid to the fulfilment of realization of information rights, protection of classified information, business secrets and other protected data groups. Service providers ensure IT security, including the integrity of electronic records, and applicability of electronic signature technology. The legislator refers to the application of electronic signature technology and the importance of compliance with the relevant security requirements.

The use of electronic signatures, according to the Act on electronic signature (hereinafter Eat.) can greatly assist in maintaining the integrity of data. However, a huge discrepancy is noticeable between theoretical principles and practice. Despite the above rules, electronic signatures are still not widely adopted and rarely usable in such systems.

Service providers shall also ensure the operation continuity and enforcement of information system collaboration requirements. As we have shown in chapter 4 and chapter 5 interoperability, i.e. cooperation between the various systems has particular importance in government information technology, as island-like systems have been developed, and over time the demand of integration has increased fairly. Negative impact of island-like development is still being felt in the area of interoperation. The continuity of operation, as one of the main requirements for IT security, including disaster and business continuity planning, is an important feature for large government databases, where data loss could and would be catastrophic.

Data transmitted to the central system profiling (analysis of user habits, personal information and direct access to meaningful case data) is not allowed according to these regulations. Compliance is ensured with the central system operator by means of technical solution. Profiling, one of the most challenging privacy issues in recent years is declared to be prohibited by a principle in Ekszt., and the information system must ensure this technically (e.g. through Privacy by Design technologies).

Use of remote services requires a face-to-face pre-registration or an equivalent measure and given that a significant number of electronic public services are administrative procedures, they need proper identification. Personal appearance and identification means a registration in governmental offices or registration by electronic signature.

Authenticity, quality, operational security and confidentiality of the data processed in electronic public services operate under the Central System must comply with defined rules. Here the act refers to Government decree no. 223/2009. (X. 14.) about the security of electronic public services. In that the requirements and procedures were determined in sections from 11 to 32. Requirements set out in the Act are detailed in the following regulations:

- Government decree 223/2009. (X. 14.) on the security of electronic public services;
- Government decree 224/2009. (X. 14.) on the central electronic system service's recipient identification and authentication services;
- Government decree 225/2009. (X. 14.) on electronic public services and their use;
- Government decree 78/2010. (III. 25.) on requirements of electronic signatures in administration and certain rules for electronic communication.

There was a bill on information security in 2009, which never came into force, but had a remarkable impact on the area. [13] The proposal was a draft legislation framework, a so called lex specialis.

The bill's scope was all IT systems and services in the Republic of Hungary, including private computers. It was applied to the operators and users, also.

According to this information systems are to be divided into 5 separate security levels. One of the factors of the grouping was storage of personal data. The groups were as follows:

- Level 1: home computer networks and individual computers connected to the Internet;
- Level 2: information systems used by every legal relationship between employer and employee, internal IT network, limited internal access non-public electronic communications services or internal network or individual computer capable to use public electronic services;
- Level 3: any public electronic services that do not handle, store, process or transfer personal identifiable information, including anonymous registration service;
- Level 4: organization providing public electronic services, application service provider and its public electronic services, regardless to personal data processing; any public electronic services that handle, store, process or transfer personal identifiable information;
- Level 5: critical infrastructure sector's computer system, closed-circuit, and public electronic network or services and information technology.

One of the most interesting questions is the mandatory audit required at level 4–5 as a means of control. According to the original intention this control would have been conducted by audit firms which are accredited previously by the National Accreditation Body for Certification Activity. Creators of the legislation could not specify whether that responsibility belongs to management systems or product certification.

Most importantly, the social impact of the law would have been significant, at least because of its wide scope. Critics had said there was lack of audit control in level 1 to 3, which made it a redundant regulation. In contrast to that, the legislation could have set the level of security requirements under other laws, because of its lex specialis character. For example, in Criminal Code Section 423 *adequate protection* is required in the case of hacking, but it was not defined earlier. The new law might have given meaningful content to it, and by doing so increasing legal certainty.

Developed Stage

Government Decision 1035/2012. (II. 21.) on Hungary's National Security Strategy requires the strengthening of the security of electronic information systems to enhance the protection of critical national information infrastructure, and the development of adequate cyber defense.

Stemming from this statement of the National Security Strategy, the Government adopted a National Cyber Security Strategy of Hungary as well. [14] The legislator took the view that recently experienced cyber wars worldwide justify the coding of a modern Hungarian Information Security Act and on 25th April 2013 a huge milestone was passed for the administrative control of information, when Act L of 2013 on electronic security of state and local government organizations was published.

The scope of the act, despite its title and scope definition in Section 2, is significantly wider than it seems to be, [15] mainly because of the following extensions: data processors of national data assets, European critical infrastructure system elements, national critical infrastructure system elements, as defined by law. These bodies can significantly extend the scope (even with private companies), so typically the public utility providers, electronic communications services, financial organizations could be included. An itemized list has not been published at the time of writing this manuscript. However, this broadening of scope might increase security in other sectors: financial security and payment transactions are also high risk areas. [16: 331]

The law prescribes the essential items known as the CIA triad in information security field: [17] confidentiality, integrity and availability as information security requirements in electronic information systems and data. The Act requires the integrity and the availability of information systems in a closed, complete, consistent way, proportionate to the risks for the electronic system and components. It is important to explicitly include the security control implementation's proportionality to risks and usage of risk assessment in the state information security requirements, because security measures are typically implemented in an ad hoc manner, to minimize security budgets.

In order to protect electronic information systems and data, proportionally to the risks, the Act states that the electronic information systems must be allocated to particular security classes. This classification is based on confidentiality, integrity and availability properties in a scale of 1 to 5 where 5 is the highest security level. From this section of the Act it seems that each part of CIA factors (confidentiality, integrity and availability) has to be evaluated separately, but in other parts of the Act we do not find this distinction.

Although the security classification depends primarily on the security classification of information, the law, in contrast to the earlier bill, does not specify what minimal security controls should be applied to data. In contrast, in Section 9 (2) it determines the minimum security level classification for a variety of organizations. This probably will have the consequence that the security needs of data will not be evaluated, instead it will be adjusted to the security levels according to the minimum-list, since the public sector tries to invest as little as possible in security. According to the Act Section 7 para 5, in *exceptional circumstances*, the manager of the organization may set a lower security class, which is another easier way to avoid spending on security. The only thing that can stop this expected downward bidding

is the strictness of National Electronic Information Security Authority based on Section 9 para 4. The authority is formed by Act Section 14 para 1.

The minimum grades in the Act per organizations according to Section 9 para 2:

- Level 1: no organizations (no requirements at this level);
- Level 2: Office of the President, Office of the National Assembly, the Constitutional Court's Office, Office of the Commissioner for Fundamental Rights, local and national self-governmental bodies, the administrative authority associations;
- Level 3: central state administration bodies, the National Judicial Office, courts, prosecutors' offices, the State Audit Office, National Bank of Hungary, the capital city and county government offices;
- Level 4: Hungarian Defense Forces;
- Level 5: data processors of national data assets, European critical infrastructure system elements, and national critical infrastructure system elements, as defined by law.

As we mentioned earlier the law does not define what these security levels are, or how should the classification be conducted and what the detailed rules for the levels are.

According to Section 11 para 1 (c), the head of the organization is obliged to appoint a person in charge of the electronic information system security, who is responsible for tasks related to the protection of electronic information systems. The list of tasks includes responsibilities of a conventional chief information security officer (CISO). Its name and definition suggesting that this person exempts the head of the organization and its employees from their security related task, but this must not be the case.

The Act set up the National Electronic Information Security Authority under the Ministry of National Development. As a specialized authority, National Security Authority deals with forensic log analysis and vulnerability testing. The existing Government Computer Emergency Response Team (GovCERT) responsibilities were handed over to different authorities. According to Section 23 the National University of Public Service develops training for those responsible for the security of electronic information systems and staff organizations.

In 2015 the legislator made a revision of the act. [18] Multiple terms and the scoping were corrected, the assignment of the security level, rules regarding authority and incident management procedure were changed. However the larges change was the unification of incident handling authority, so the Government Incident Response Team under the Special Service for National Security has taken back the event handling responsibilities.

Consequences

The article showed the major issues of information security with historical background. It also showed the trend of more definite legal regulation, even with inception of technical standards in legal regulations. Due to the wide range of important legislation in the long-term wide social effects and improvement of information security awareness are expected. Probably the standard-based (e.g. ISO 27001 or COBIT) systems will multiply, given the fact that the organizations will already comply with the security rules. This trend is also perceptible in Hungarian legislation, which was also detailed in the article with the alignment of national cybersecurity strategy. This had three phases until now: early strategies and legislation of 1989–2008, Interim transition strategy of 2009–2012, and the latest, developed information security strategy from 2012. This last one passed a huge milestone in 2013, when the

Hungarian Act L of 2013 on Electronic Security of State and Local Government Bodies was introduced, which is already being applied and revised.

This change in strategy and regulations will result in greater security and the national security risk in the area of information and communication technologies will decrease in the long term. The Act is a good step in the direction of the appropriate level of government information security, but it still provides loopholes from the application of the rules.

References

[1] KÖPECZI B. (Ed.) et al.: *Az embergéptől a gépemberig*. Budapest: Minerva, 1974.

[2] KITA, C. I.: J.C.R. Licklider's Vision for the IPTO. *IEEE Annals of the History of Computing*, 25 3 (2003), 62–77.

[3] SASVÁRI P., NEMESLAKI A., RAUCH, W.: Old Monarchy in the New Cyberspace: Empirical Examination of Information Security Awareness among Austrian and Hungarian Enterprises, *AARMS*, 14 1 (2015), 63–78.

[4] GORGE, M.: Cyberterrorism: hype or reality? *Computer Fraud and Security*, 2 (2007).

[5] NETANJAHU, B.: *Harc a terrorizmus ellen*. Budapest: Alexandra, 1995.

[6] TIEFENBRUN, S.: A semiotic approach to a legal definition of terrorism. *ILSA Journal of International and Comparative Law*, 9 2 (2003), 358–402.

[7] HAIG ZS., KOVÁCS L.: New way of terrorism: Internet- and cyber-terrorism. *AARMS*, 6 4 (2007), 659–671.

[8] SZÁDECZKY T.: IT Security Regulation and Practice in Hungary. In. POROSZLAI Á. (Ed.), *Proceedings of the New challenges in the field of military sciences 2010*. Budapest: ZMNE, 2010.

[9] *Hungarian Act CXII of 2011 on informational self-determination and freedom of information.*

[10] JÓRI A.: *Adatvédelmi kézikönyv. Elmélet, történet, kommentár*. Budapest: Osiris Kiadó, 2005.

[11] DEDINSZKY F.: *Informatikai biztonsági elvárások*. Budapest: MeH–EKK, 2008.

[12] *Hungarian Act LX of 2009 on electronic public services*.

[13] MEH: *Draft of act on information security*, Budapest: MeH, 2009.

[14] *Hungarian Government decision 1139/2013. (III. 21.).*

[15] MUHA L., KRASZNAY Cs.: Kibervédelem Magyarországon: áldás vagy átok? *HWSW online*, 5026 (2013).

[16] CSER O.: The Role and Security of Money from the Aspect of Cyber Warfare. *AARMS*, 14 3 (2015), 331–342.

[17] *Hungarian Act L of 2013 on Electronic Security of State and Local Government Bodies.*

[18] *Amended by Hungarian Act CXXX of 2013.*