ISSN 1392–6195 (print)
ISSN 2029–2058 (online)
JURISPRUDENCIJA
JURISPRUDENCE
2011, 18(2), p. 703–724.

PRECONDITIONS FOR LEGAL REGULATION OF PERSONAL IDENTIFICATION IN CYBERSPACE

Darius Štitilis

Mykolas Romeris University, Faculty of Social Informatics,
Department of Electronic Business
Ateities g. 20, LT-08303 Vilnius, Lithuania
Telephone (+370 5) 271 4572
E-mail stitilis@mruni.eu

Paulius Pakutinskas, Inga Dauparaitė

Mykolas Romeris University, Research Center
Ateities g. 20, LT-08303 Vilnius, Lithuania
Telephone (+370 5) 271 4571
E-mail: paulius.pakutinskas@teo.lt; inga.dauparaite@hipotekosistaiga.lt

Marius Laurinaitis

Mykolas Romeris University, Faculty of Economics and Finance Management,
Department of Banking and Investments
Ateities g. 20, LT-08303 Vilnius, Lithuania
Telephone (+370 5) 271 4550
E-mail laurinaitis@mruni.eu

Received 26 April, 2011; accepted 17 June, 2011

Abstract. *The article analyses legal preconditions for personal identification in physical and electronic space (hereinafter – cyberspace). Analysis of legal governing of identification in physical space is followed by the analysis of the same in cyberspace. Compulsory*

© Mykolo Romerio universitetas, 2011
© Mykolas Romeris University, 2011
ISSN 1392-6195 (print), ISSN 2029-2058 (online)
http://www.mruni.eu/lt/mokslo_darbai/jurisprudencija/
http://www.mruni.eu/en/mokslo_darbai/jurisprudencija/

elements of identification in physical space and compulsory and non-compulsory elements of identification in cyberspace are provided which leads to conclusions about problem aspects concerning personal identification in cyberspace and related legal governing.

This scientific article consists of four main chapters. The first chapter „Identity and Personal Identification" looks into identity, its content and elements alongside with personal identification. The second chapter „Personal Identification in Physical Space" scrutinizes legal preconditions of identification in physical space in Lithuania. The third chapter „Personal Identification in Cyberspace" looks into elements of legally regulated and non-regulated personal identification in cyberspace and discusses identity of a person in cyberspace. The fourth chapter „Electronic Identity of a Person and Legal Regulation" analyzes and systematizes elements of electronic identity of the person and presumes their reliability and mandatory legal governing.

Keywords: *personal identification, identification in cyberspace, identity, physical space, cyberspace.*

Introduction

Relevance of the theme: personal information, which is often used in the process of identification, is in particular important in the social environment. This information is also used in cases where personal presence of a person is not possible, i.e. in cyberspace[1]. Personal information is provided while using services of electronic government, electronic commerce and other services.

Personal identification in physical space[2] is based on documents establishing identity of a person. However, an increasing supply of services in an electronic form causes another identification need and there evolve new personal identification techniques, therefore, it is important to analyse legal preconditions of personal identification in physical space and in cyberspace while evaluating elements of identification in cyberspace and their influence on social and legal relationships. In order to understand what forms our identity and what its elements are in physical and cyberspace, it is necessary to define the concepts, clarify for ourselves the content of personal identity and means for and features of identifying a person. It is also important to determine what data are used to verify personal identity in physical and cyberspace, which documents lay down the said data and what requirements are imposed on them.

Novelty of the theme: novelty of the theme manifests itself in that personal identification in physical and cyberspace is for the first time analysed through a comparative aspect. Based on executed research authors raise scientific discussion on the influence of legal indefiniteness of identification in cyberspace on social and legal relationships, including electronic commerce and theft of identity in cyberspace.

1 Cyberspace is treated by the authors broader than in definitions (Cyberspace is an electronic medium of computer networks in which online communication takes place) – this encompasses not only "online" relationships but any electronic medium as well (for example, electronic information stored in different electronic media (USB media and etc)).

2 Physical space is understood by the authors as public relationships arising in non-cyberspace.

Purpose of the scientific article: analysis of preconditions for personal identification in physical and cyberspaces.

Object of research: personal identification in physical and cyberspace.

Methods of research: several different methods were used in the research: empirical method for the analysis of legal documents which was used for the setting of legal governing that is in force in Lithuania with respect to personal identification in physical and cyberspace. Legal regulatory acts of the Republic of Lithuania have been examined. This method allows, upon examining official documents, to define correctly and describe a valid legal governing of a respective relationship and, upon additionally investigating previous and subsequent editions of legal regulatory acts, to reveal historical change of this governing. Investigating similarities and differences of the ways and measures of personal identification in electronic and physical space and other questions of problem, the authors have resorted to theoretical methods. One of them is a comparative method. The aim of comparing measures and ways of identification in physical and cyberspace is to interpret differences in reliability and safety of personal identification. Another theoretical method that has been deployed to research problems of safety in personal identification in cyberspace is the method of analogy. Authors researched not only measures and ways of personal identification provided for by the laws, but all other ways and measures broadly applied for personal identification in cyberspace. This method, together with the comparative method, allows to explore a relationship between reliability and safety of broadly used personal identification ways and measures provided for by the legal norms and to make conclusions concerning the need for legal regulation of public relationships concerned. Using sources of scientific literature, authors deployed a deduction method which enabled arriving at sufficiently reliable conclusions. To examine the concepts authors used the latest research literature and vocabularies.

Level of investigation of the theme: scientists in Lithuania are more extensively analysing themes relating to biometrical personal data; personal identification is examined while using recognition of the person's face and eye iris. Dissertations have been defended in this area (Justas Kranauskas, Andrej Kisel), but the field of legal aspects in creation and use of identity in cyberspace has been left aside. Foreign authors pay bigger attention to threats which are present in cyberspace – thefts of identity and other legal offences in cyberspace (Kai Rannenberg, Denis Royer, André Deuker, Nir Kshetri), whereas investigations of legal governing of personal identification in cyberspace are still lacking.

The article will analyse mechanisms for developing legal identity and will review measures that confirm personal identity in physical space. Apart from state institutions which are authorised to store identity data in respective registries, the article will also analyse relevant personal electronic identity.

1. Identity and Personal Identification

Identity can be perceived differently, as national identity, regional identity, professional identity, and personal identity, but these concepts are less of a legal nature.

Such identity encompasses personal self-perception, in relationship with another group or groups. Such identity could be called social identity. Social identity includes identification in a team or group and belonging to the nation and class; it depicts belonging to ethnical and religious groups; cultural identity is also attributed to such identity.[3]

Another important identity distinguished in scientific sources is personal medical identity. It is the most accurate identity unambiguously associated with a person. It can be characterized as personal data and information which is used to establish personal identity, for example, an image of a person, finger prints, detailed description of a person (body and face), individual's DNR data and other specific features of the body (malformations, physical disabilities)[4](as additional identifiers).

Personal identity relevant to this particular scientific research would be that identity which has been approved by the state. Such identity is provided in the form of entries in respective registries. Information compiled and stored on a person in state registers can be called legal personal identity, because it has been created based on the procedure specifically laid down in legal norms. I.e. while granting to a person digital codes (personal codes, social insurance codes, codes identifying an individual and etc) and while making entries in state registries directly related with a person (name, surname, birth date and etc).[5] It can be stated that such identity is created only by the state and it may differ from personal social identity. Presently the state, while creating personal identity, applies not only the above-mentioned method of entry formation, but also a modern medical–biometric method which allows avoiding mistakes and falsifications, because, in fact, it is impossible to appropriate personal medical identity. There may and does exist identity which is not created but recognized by the state (for example, safe identification via the banking system to receive and manage services from the State Tax Inspectorate).

The so-called contractual identity is also possible when an individual is identified based on agreed identification methods and measures instead of state-approved methods and measures. Such identity has not been legally regulated and therefore may be unreliable; however, such identification methods are quite often acceptable for both parties. A more detailed examination of the ways of creating and establishing electronic identity reveals differences in defining them in different states. Electronic identity in the U.S.A. is a unique naming of an individual. Since names of individuals are not necessarily unique, electronic personal identity must contain enough additional information in order to create an entirely unique electronic identity.[6] Institutions from New Zealand provide a omewhat different definition of electronic identity: electronic identity is an established group of features and/or data associated with a specific person.[7] However, no indication is

3 Alcoff, L.; Hames-Carcia, M.; Moya, P. M. L. *Identity Politics Reconsidered*. Palgrave Macmillan, Basingstoke. 2006.

4 "Medical ID". Last, J. M. *A Dictionary of Public Health*. Oxford University Press, Inc., 2007.

5 Cane, P.; Conaghan, J. *The New Oxford Companion to Law*. Oxford University Press Inc., 2006.

6 Electronic Authentication Guideline. Recommendations of the National Institute of Standards and Technology. NIST Special Publication 800-63 Version 1.0.2. [interactive]. [accessed 23-03-2011]. <http://www.usda.gov/egov/egov_redesign/intranet/eauth/SP800-63V6.pdf>; p. 16.

7 Guide to Authentication Standards for Online Services. State Services Commission, June 2006, Version 1.0. Crown Copyright. [interactive]. [accessed 23-03-2011]. <http://www.e.govt.nz/plone/archive/services/authentication/standards/guide-to-authentication.1.html>; p. 33

provided whether such identity can be compared to legal identity (except when respective technologies and decisions of electronic signature are used) and what data should be used in order to create unique personal electronic identity.

It is namely the entirety of the data used to identify a person which makes our identity. In a vocabulary of international words identicalness is equalled to identity, where identity is identicalness, indefiniteness and individuality of something[8]. In the latest vocabulary of the Lithuanian language identity means equality of an object to itself or another object, equivalence, sameness.[9]

So how is identity regulated in physical and cyberspace?

2. Personal Identification in Physical Space

Identification in physical space is carried out while using one of the mandatory identification measures – an appropriate personal document. Such identification, while using official state-issued documents, may be termed as official identification. Another identification in physical space is also possible – using documents issued by other than state subjects (for example, a certificate of an employee), however, this identification is local and will not be analysed in this research article.

It should be mentioned that identification in physical space takes place only in certain projected circumstances (for example, when a state authoritatively prescribes identification necessity) and relatively; identification of relationships as such is not necessary for the majority. We can provide a case of a simple shop where no personal identification is required while buying a commodity, because the transaction and payment here are immediate, i.e. they occur at the time of buying a commodity.

Nevertheless, when it is needed to identify a person, most often official state-approved documents are used. It can be stated that namely the data consolidated in official personal documents form individual's identity in physical space. However, how does identity appear in physical space and who does verify this identity?

2.1. Elements of Physical Personal Identity Consolidated in the Register of the Republic of Lithuania

The process of granting physical personal identity starts right from the beginning of the birth of a person. In Lithuania a birth of a child must be declared and registered with the Civil Registry Office no later than three months later.[10] Registering of the birth requires submission of a child birth certificate issued by a health care establishment or doctors consultation commission, and said certificate is namely that document whereby a fact and time of a child's birth is confirmed[11]. This child birth certificate issued means

8 „Identity". Guide to Authentication Standards for Online Services. State Services Commission, *supra* note 7.

9 „Identity". *Dictionary of the Lithuanian Language*. Vilnius: Institute of the Lithuanian Language, 2005.

10 22 July 2008 Order of the Minister of Justice of the Republic of Lithuania No 1R-294 „On the Ammendment of 19 May 2006 Minister of Justice Order No 1R-160 „On the Approval of the Rules of the Civil Registry Office"". *Official Gazette*. 2008, No 88-3541; part 29.

11 Identity appears namely from this moment.

the first recorded personal data which later are used while entering a birth entry and issuing a birth certificate.[12]

Upon birth of a child, a Civil Registry Office forms a new entry in the main data base of the population of the Republic of Lithuania – Residents‘ Register. The institution assigned to collect, accumulate, process and store personal data (about citizens of the Republic of Lithuania, persons without citizenship or citizens of other countries declaring their residence in Lithuania or registering changes in the personal civil status in the institutions of the Republic of Lithuania), provide these data for the authorities of the Republic of Lithuania, local municipal institutions, state registers and other legal and natural persons following the procedure laid down by the laws and other legal acts is – Residents‘ Register Service under the Ministry of the Interior of the Republic of Lithuania. This institution manages the Residents‘ Register.[13]

The Residents‘ Register Service operates key personal identity data intended for the identification; this is the only institution which has been assigned the function of compiling all the data by means of which a personal identity can be formed (Table 1).

Table 1. Personal identity data operated by the Residets` Register, composed by authors

PERSONAL DATA (MAIN)	OTHER PERSONAL DATA (INFORMATION OF SOCIAL CHARACTER)	INFORMATION ON PERSONAL DOCUMENTS
• Personal code; • Name (names); • Surname (surnames); • Gender; • Date of birth; • Citizenship (citizenships); • Place of birth; • Signature; • Date of death;	• Place of residence, date of arrival to the place of residence; in case of departure abroad, – place (state) and date of departure; in case of permanent residence abroad, – a state; in case of having no place of residence, – municipality of residence; • Personal codes of parents, children and spouses; if no personal codes have been granted, - other personal data substantiated with documents and specified in the provisions of the register; • Nationality (data on nationality are provided from the register only following the procedure laid down by the Law on Legal Protection of Personal Data of the Republic of Lithuania); • Family situation and date of its change;	• Data of personal documents (type, code and name of the issuing state, series and number, cause of issue (change), date of writing and date by which a personal document is valid, date of issue, state of validity (invalidity), cause and date of invalidity, information if a personal document has been returned or not returned); • Data on requests to receive documents (registration number and date, code and name of the establishment which accepted a request); • Data on the entries in the civil situation acts (type, grounds of entry, place and date of entry, number, and grounds for amendments, marking on the issue of the certificate, place of death, comments entered in the entry).
PERSONAL BIOMETRIC DATA[14]		
• Facial image • Finger prints		

Drafted based on: Law on the Population Register. *Official Gazette*. 1999, No 28-793.

12 22 July 2008 Order of the Minister of Justice of the Republic of Lithuania No 1R-294 „On the Ammendment of 19 May 2006 Minister of Justice Order No 1R-160 „On the Approval of the Rules of the Civil Registry Office““. *Official Gazette*. 2008, No 88-3541; part 29.

13 Law on the Population Register of the Republic of Lithuania. *Official Gazette*. 1999, No 28-793; Article 3.

14 Final list.

Personal data accumulated in the Population Register form the content (elements) of identity, however, all this data is not needed in everyday activity of a person. These personal data accumulated in the Population Register are used while issuing to persons respective official documents by means of which a physical person can be identified in physical space.

2.2. Documents Verifying Personal Identity in Physical Space

Birth certificate is the first personal identity document which is issued to a person. A personal document is a document issued to a person by the state or local municipal institution in which data on this person are included in the manner specified by the laws and other legal acts of the Republic of Lithuania.[15] A birth certificate verifies origin of the child – parents of a child are verified by a birth entry entered in the civil marriage establishment and a birth certificate issued on the basis of the birth entry.[16]

Data on the parents of a child in the birth certificate are entered based on personal identity documents of the parents of a child checked against the data of the central base of the Population Register. Other most important elements of identity like a name, surname, personal identification number are established as follows: name (two names) is (are) granted by the agreement of the parents. If parents fail to agree on the name or surname of a child, registration of the child's birth is postponed until the submission of a court decision to grant a name (surname) to a child. If parents of a child are married and their surnames and nationalities are the same, a child is given his parents' surname taking into account his gender.[17] A personal identification number is also allocated to a child in a prescribed manner. It must be emphasized that a personal identification number allocated to a person is unique, it can not be changed and it is entered in personal documents.[18] Elements of personal identity can change, however, once generated, a personal identification number remains for ever.

When a person reaches a respective age of a subject, the main documents verifying personal identity will be primarily used to confirm personal identity – *a personal identity card or a passport*[19]. It should be noted that both a personal identity card and a passport are principal documents of a citizen of the Republic of Lithuania[20] which verify his

15 Law on the Population Register of the Republic of Lithuania. *Official Gazette*. 1999, No 28-793; paragraph 11 of Article 4.

16 Civil Code of the Republic of Lithuania. *Official Gazette*. 2000, No 74-2262; Article 3.138.

17 *Ibid*.

18 Law on the Population Register of the Republic of Lithuania. *Official Gazette*. 1999, No 28-793; paragraph 3 of Article 8.

19 By 23 October 2010, a passport of the Citizen of the Republic of Lithuania was a mandatory personal document, whereas an identity card was optional. But as of the said date, both a passport and an identity card has become alternatively selected documents identifying personal identity. In the opinion of authors, a possibility of selecting only a passport causes preconditions for a slower spread of an electronic signature.

20 These documents are recognized by all state institutions and private economic entitities.

personal identity and citizenship and are intended for use in the Republic of Lithuania[21]. Only the procedure for recognizing these documents abroad is different. An identity card, issued since 2009, is bilaterally recognized in foreign states as a document identifying personal identity (their list is provided by the Migration Department under the Ministry of the Interior of the Republic of Lithuania).[22] Menawhile, the passport is intended to travel to all foreign states.[23] Therefore, states with which Lithuania has not agreed to acknowledge identity cards as documents verifying personal identity, establish personal identity based on another most important personal document – the passport.

Less data are indicated in a personal identity card than registered in the said Population Register (Table 2). The quantity of the data elements is sufficient to identify a specific person.

Table 2. Personal identity data indicated in a personal identity card, composed by authors

PERSONAL DATA	DATA ON THE DOCUMENT
• Name (names). • Surname. • Gender. • Date of birth. • Personal identification number. • Citizenship. • Facial image. • Citizen's signature.	• Date of issue of a personal identity card. • Name of the establishment which issued a personal identity card. • Date by which a personal identity card is valid. • Number of the personal identity card.
ELECTRONIC RECORDING	
• Facial image. • Finger prints. • Certificate of personal recognition in cyberspace. • Qualified certificate.	

Drafted based on: Law on Identity Cards of the Republic of Lithuania. *Official Gazette*. 2001, No 97-3417.

Personal data, which are recorded in a passport, insignificantly differ from the data which are provided in an identity card (Table 3). Differences have been supported by an additional function of the passport provided for by the law as a document identifying personal identity while travelling to foreign states, for example, an entry on the place of residence and etc.

21 Law on Identity Cards of the Republic of Lithuania. *Official Gazette*. 2001, No 97-3417, paragraph 1 of Article 2; Law on Passports of the Republic of Lithuania. *Official Gazette*. 2001, No 99-3524, paragraph 1 of Article 2.

22 Personal identity card [interactive]. [accessed 23-03-2011]. <http://www.pasienis.lt/lit/asmens tapatybės korteliu_galiojimas_ir_/132>.

23 Law on Passports of the Republic of Lithuania. *Official Gazette*. 2001, No 99-3524; Article 2.

Table 3. Personal identity data recorded in a passport, composed by authors

PERSONAL DATA	DATA ON THE DOCUMENT
• Name (names). • Surname. • Gender. • Date of birth. • Place of birth (name of the state is entered). • Personal identification number. • Citizenship. • Facial image • Citizen's signature.	• Date of passport's issue. • Name of the establishment which issued a passport. • Date by which a passport is valid. • Passport number.
ELECTRONIC RECORDING[24]	
• Facial image. • Finger prints.	

Drafted based on: Law on Passports of the Republic of Lithuania.

One more document, which is practically used as an identity verification document, is a *driver's licence of a new version of the Republic of Lithuania*. A driver's licence is a document issued following the procedure laid down by legal acts whereby a personal right to drive a motor means of transport of a certain category is confirmed and driving conditions are specified[25]; the provided definition does not name it as a document verifying personal identity, however, a review of the agreements on supplying services by different financial institutions operating in Lithuania established that, for example, all commercial banks of Lithuania accept a driver's licence issued after 31 December 2001 (of a new version) as an identity verifying document[26]. The rules of the banks define a personal identity document as an *attesting, confirming, acceptable and valid* document containing a photograph, signature, name, surname, and personal identification number. Therefore, banks treat the driver's licence as a document attesting to and confirming personal identity.

The procedure of issue of the driver's licence of the new version specifies that an applicant submitting a request must additionally provide to an authorized person a valid personal document – a personal identity card or a passport; documents and date on the place of residence declared by an applicant are checked in the Population Register of the Republic of Lithuania.[27] Personal identity is established during the said procedure, and required personal data are entered in the driver's licence (Table 4). Scope of data

24 Final list.

25 Law on Safe Traffic on Roads of the Republic of Lithuania. *Official Gazette*. 2000, No 92-2883; Article 2.

26 This is indicated in general rules on services of commercial banks.

27 Order No 1V-328 „On the approval of rules to issue driver's licence of motor means of transport" issued by the Minister of the Interior of the Republic of Lithuania on 10 September 2008. *Official Gazette*. 2008, No 106-4060; Paragraph 2 of Article 13.

elements is conditioned by the main function of the driver's licence – to attest to the right granted to drive a respective means of transport.

Table 4. Personal identity data indicated in a dricer`s licence, composed by authors

PERSONAL DATA	DATA ON THE DOCUMENT
• Surname of the certificate bearer. • Name(s) of the certificate bearer. • Personal identification number of the certificate bearer. • Facial image of the certificate bearer. • Signature of the certificate bearer.	• Date and place of birth of the certificate bearer. • Date of issue of the certificate. • Date of expiry of the certificate. • Name of the institution which issued a driver's licence. • Certificate number. • Codes of categories of the means of transport which the owner has the right to drive.

Drafted based on: 20 November 2008 Order No 1v-411 of the Minister of the Interior of the Republic of Lithuania „On the amendment of 14 June 2005 Order No 1v-186 of the Minister of the Interior of the Republic of Lithuania „On the description of the driver's licence's form and on the approval of the mandatory form".

Data recorded in the driver's licence correspond to personal data recorded in lawfully recognized personal identity documents, and their veracity is conditioned by the check of the data carried out in the Population Register of the Republic of Lithuania. A driver's licence of a new version of the Republic of Lithuania is a technically secured document and the legal status in the Register of Authentic Identity and Travel Documents of the European Union has been described as follows: „A driving licence issued to persons with legal residence: LTU – Lithuania. The document is used *to establish identity of the bearer* in the territory of that country, but it is not a proof of the bearer's citizenship."[28], therefore should not be discriminated by institutions of member states in identifying personal identity. The same position is taken by the Ministry of the Interior of the Republic of Lithuania which has publicized a notification stating: „Ministry of the Interior proposes for state institutions and establishments to service applicants upon submitting by them, apart from a passport or personal identity card, also another document confirming personal identity (i.e. driver's licence)."[29] It is indicated that this is a request of the citizens, therefore, other ministries have been addressed to review and, if appropriate, adjust legal acts that are within their competence and to establish which documents proving personal identity must be submitted in order to receive different services. This proposal is rational bearing in mind reliability of such a document and veracity of its data. Due to these reasons, a current driver's licence is accepted by financial institutions as a valid personal document.

28 European Council, LTU-FO-02002 [interactive]. [accessed 23-03-2011]. <http://www.consilium.europa.eu/prado/LT/2812/docHome.html> .

29 It is proposed to treat the driver's licence as a document confirming personal identity [interactive]. 2010-04-30 [accessed 23-03-2011]. <http://www.vrm.lt/index.php?id=131&backPID=1340&pS=1270069200&pL=2591999&arc=1&tt_news=2466&>.

There is one more document which confirms personal identity in Lithuania and that a person for whom it was issued serves in a public service that is a *certificate of a civil servant*. However, this is a document of special purpose issued to civil servants only, therefore we are not going to analyse it or derivative personal documents in more detail[30]; they contain personal data, but under legal acts in force they usually can not be used as a legal measure to confirm personal identity (except a possibility of identification in local systems).

Thus, we have discussed the most important lawfully accepted documents which prove personal identity in physical space. Such documents are issued only by institutions authorized by the State and they are the only legal measure to identify identity in Lithuania. Each of this documents is intended for a certain specific purpose, therefore, these documents do not overlap[31] and they provide as much data as is necessary for a specific legal relationship.

3. Personal Identification in Cyberspace

Due to the development of electronic services, states faced a need to identify persons both in physical and cyberspace. Notwithstanding a document confirming personal identity, the content of identity in physical space is similar. Meanwhile, it is impossible to provide in cyberspace a non-electronic, official and traditional document identifying personal identity, however, persons face a very frequent need to confirm their identity in this media.

It must be mentioned that, in comparison with physical space, the quantity of identification in cyberspace is relatively bigger. Therefore, one needs to use personal information in cyberspace much more often and this alone conditions a bigger number of identity thefts[32].

Electronics space with respect to identification is somewhat specific in that one does not need physically to be in a respective geographical place in order to identify oneself. Cyberspace enables persons to carry out effective actions from a distance. Examples of effective actions can be transmission, accumulation, processing and use of electronic information, therefore, persons need not to be in a specific location to make use of such information or perform an effective action.

Then there arises a question what identity verification measures are used in cyberspace? And what are official state-approved identification methods?

30 Student certificate, pensioner's certificate, employee's certificate and etc.

31 Except the case of a passport and card.

32 Higgins, H. E. *Cybercrime: An Introduction to an Emerging Phenomen*. McGraw-Hill, 2010, p. 74.

Majority of systems of electronic services use similar personal identification means. Generalisation and grouping allows distinguishing the following most important personal identification elements and identification examples in cyberspace (Figure 1):[33]

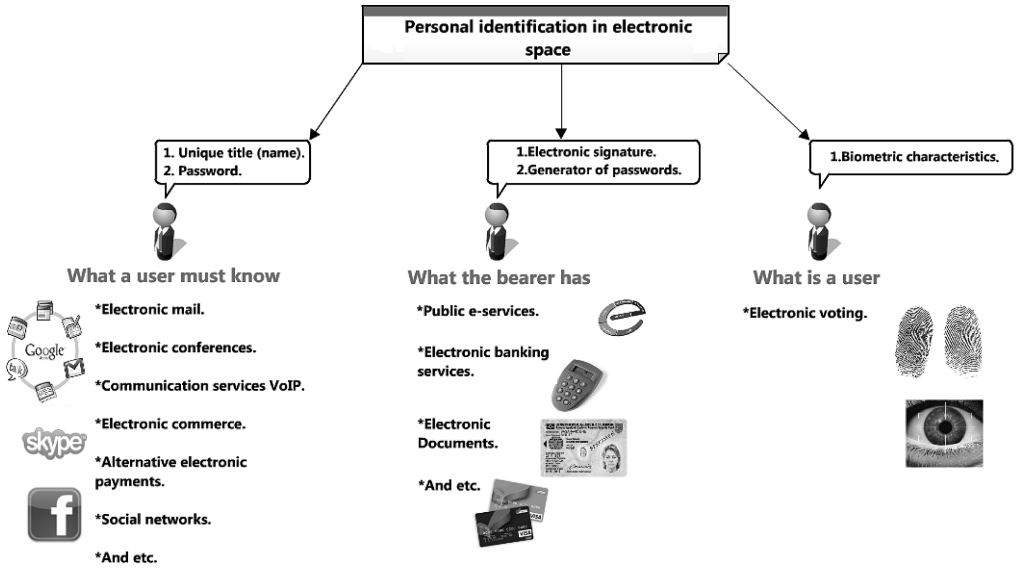


Figure 1. The main electronic identity elements, designed by authors

3.1. Identification Pursuant to What a User must Know

As indicated in Figure 1, a person can be identified in cyberspace by a unique title (name) and password. Names of persons in physical space can repeat, however, personal identity in the same electronic system must be identified using a unique identifier. This is conditioned by specificity of the very systems, there can not be the same names describing different persons. A chosen password is usually a line of characters. Reliability of such a method depends upon the level of security of the information system. Short passwords are insecure, long and complicated passwords are difficult to memorize. Safety of such systems depends upon users themselves. If users will use their identification elements insecurely, such identity will be an easy target for appropriation. Majority of known electronic services are based on this principle of identification:

- Communication services – electronic mail, electronic conferences, communication services VoIP and etc.

33 Electronic Authentication Guideline. Recommendations of the National Institute of Standards and Technology, *supra* note 6.

- Electronic commerce – electronic shops, other subjects providing electronic services, alternative electronic payments and etc.
- Social networks, virtual communities and etc.

If we analyse the same social relationships in physical space, we would notice that identification in physical space in similar cases might not take place at all. Concerning transactions, there are many momentary transactions in physical space when identity of physical person is not relevant (important is the payment made in such a monetary transaction). Meanwhile, momentary transactions in cyberspace are in fact not present, thus, even the smallest operation requires personal identification. And as we see, such identification is often a matter of agreement.

However, can such identity be called real? It should be mentioned that the state does not regulate this identification. This means that such identification mechanism is a matter to be agreed between a service provider and a client. Often in practice unique names chosen by persons have nothing to do with real identities. Users are not obligated to confirm their real identity while registering in such systems, but identity thus generated becomes personal data protected by legal acts. It's not seldom that an email address turns into one of the most important elements identifying identity in cyberspace. However, email service providers do not check personal identity upon registration thus creating favourable conditions for identity counterfeiters. Conditional simplicity of electronic mail identification systems, possibility to appropriate user names and passwords indicate a serious problem – loss of electronic identity.[34]

Similarly, problems arise due to fast spread of social networks in the Internet. They enable transfer of one's identity and social relations into cyberspace. Social networks are more than just a means of communication becoming into a medium for running business and developing working relationships where each electronic identity associates with genuine personal identity – an existing individual. Persons register and transfer their personal data into such networks, however, they have no guarantees against appropriation of their identity. Registration to such social networks is based on electronic mail, namely an email and chosen password becomes electronic identity. However, failure to apply reliable identification means and conditional simplicity of registration increase a risk of using social networks for criminal activity. In September 2010, criminals appropriated identity of the head of Interpol in a social network „Face book". Two false profiles have been created in his name, criminals used them to get information on operations carried out by international police agency.[35] Security of social networks and simplicity of registration are becoming a global problem.[36]

---

34 Google targeted in e-mail scam [interactive]. [accessed 23-03-2011]. <http://news.bbc.co.uk/2/hi/technology/8292928.stm>.

35 Interpol chief has Facebook identity stolen [interactive]. [accessed 23-03-2011]. <http://www.networkworld.com/news/2010/091910-interpol-chief-has-facebook-identity.html>.

36 First INTERPOL information security conference to provide global platform for preventing and detecting high-tech crimes [interactive]. [accessed 01-12-2010]. <http://www.interpol.int/public/ICPO/PressReleases/PR2010/PR070.asp>.

3.2. Identification Pursuant to What the Bearer Has

This principle underlies recognition of the client using available measures: electronic signature (verified with electronic certificate), code generators and code tables. As compared with physical space, this is namely a state-regulated (or recognized) identity.

First of all, we will discuss electronic identity which is subject to the procedure of imperative regulation by the state. A lawfully recognised and regulated method of personal identification in cyberspace is an electronic certificate and electronic signature. Electronic certificate means an electronic attestation, which links signature-verification data to a signatory and confirms or allows establishing the identity of that signatory.[37] Electronic signature means data, which are inserted, attached to or logically associated with other data for the purpose of confirming the authenticity of the latter and (or) identification of the signatory.[38] Electronic certificate as a means of confirming personal identity in cyberspace is in more detail described by the Law on Identity Cards of the Republic of Lithuania: Certificate of personal recognition in cyberspace means an electronic attestation with inserted and indicated technical data set by the Minister of the Interior which confirms or allows to establish personal identity in cyberspace.[39] The purpose is clearly indicated – to establish personal identity; personal data entered in the certificate correspond to the data of the identity card: name (names), surname, gender, date of birth, personal identification number, citizenship.[40] A personal identity card is a document which can prove your identity in physical and cyberspace: „A personal identity card can be used to confirm or establish personal identity in cyberspace and to sign electronic data (issued as of 1 January 2009)".[41]

There are three providers of services of electronic certificates and qualified electronic signatures in Lithuania.[42] All of them have the right to create valid and approved personal electronic identity[43], which legally is identical to physical identity confirmed by valid personal documents. However, only state institutions, which guarantee authenticity and veracity of these documents, have the right to issue said personal documents. Meanwhile, electronic personal identity can be created by non-state institutions too. Of course, this should not suppose an opinion that it is not safe, but if a state is responsible for the generation of the content of individuals' identity and accumulation and storage of such data, wouldn't it be right to apply the same mechanism for the creation of electronic identity too?

---

37 Law on Electronic Signature of the Republic of Lithuania. *Official Gazette*. 2000, No 61-1827; paragraph 4 of Article 2.

38 *Ibid*.

39 Law on Personal Identity Cards of the Republic of Lithuania. *Official Gazette*. 2001, No 97-3418; paragraph 1 prim of Article 1.

40 *Ibid*.

41 *Ibid*.

42 UAB "Skaitmeninio sertifikavimo centras", VĮ "Registrų centras", Residents Register Service at the Ministry of the Interior of the Republic of Lithuania.

43 It should be mentioned that it is possible to have more than one electronic signature (based on different systems), differently from physical space where it is never allowed to legally have two originals of the same document.

An electronic personal certificate has been generated based on mathematical algorithms, its reliability is guaranteed by approved standards. Theoretically, such a certificate is more secure than any personal document. However, its reliability depends upon the person to whom it belongs, because the certificate itself is protected by the password whose loss poses a risk of someone being able to make use of electronic certificate to identify oneself as another person. Absence of physical contact and probability of losing a certificate media make the risk even higher.

Discussed electronic identity supported by certificates is extensively used by persons seeking to receive electronic services provided by state institutions. Institutions identify persons by their electronic certificates and by something more. Rules for the functioning of the interoperability system of information systems of public administration institutions provide that while connecting to information systems of public administration institutions, personal identity can be established using an electronic signature, approved by a qualified certificate, and electronic banking systems.[44]

State-recognised electronic identity is also possible. Electronic banking services use their own identification system which connects two elements of identification in cyberspace: „What is known" and „What is possessed" and which is accepted by a state. I.e. this electronic identity has the legal power of law, because it rests on the provision of paragraph 3 of Article 8 of the Law on Electronic Signature of the Republic of Lithuania: "In all cases, the electronic signature shall have the legal power laid down in paragraph one of this Article, provided that the signature users shall reach an agreement among themselves."[45]. Namely agreement between the bank and the client that a respective bank system conforms to the features of the safe system and the above-mentioned legal norm of the law and identification based on this system suppose the fact that the said identification system is recognised by the state.

Means of protection used by the bank to identify the clients:[46]

1. Recognition code means a unique sequence of digits which is used to establish personal identity while registering in the system.

2. Password means a unique sequence of digits which is used to confirm personal identity while registering in the system; the bank recommends creating a password from letters, digits and symbols which should be subject to regular alteration.

Means of recognition used by the bank to identify persons:

1. A card of passwords indicating numerated passwords which are entered in the system at the beginning of the communication session or while confirming operations.

2. A generator of passwords which, under a special algorithm, creates a unique password – sequence of digits each time while registering in the system.

---

44 1 December 2008 Order of the Director of Information Society Development Committee at the Government of the Republic of Lithuania „Rules for the functioning of the interoperability system of information systems of public administration institutions". No T-228. *Official Gazette*. 2008, No 145-5850; Part IV, paragraph 13.1.

45 Law on Electronic Signature of the Republic of Lithuania. *Official Gazette*. 2000, No 61-1827; paragraph 3 of Article 8.

46 Drafted in accordance with agreements on supplying services by commercial banks operating in Lithuania.

A client selects a recognition measure allocated to a user at his own discretion. A user must know his unique number in the system, a password which he constantly changes and he must have one of the recognition measures. Once a generator of the passwords has been chosen, contrary to the card of passwords, digital formations received by him never repeat.

Authenticity of the user is deemed to be confirmed if the user correctly used bank-allocated recognition and protection measures at the beginning of the communication session and if the bank received user's information about his registration in the system. The bank recognizes and deems notifications received via the bank system on the use of the funds in the accounts of the clients, conclusion of agreements, amendment of the conditions of the agreement, supplementation of the agreement, extension of the term or termination of the agreement and other information as signed and confirmed if at the beginning of the communication session correct recognition and protection measures have been indicated, in other words, the bank recognizes this identification system as an electronic certificate and treats all confirmed documents equivalent to documents executed in writing. As mentioned, such a possibility is granted to the banks by the Republic of Lithuania Law on Electronic Signature; therefore, client identification systems used by the banks for electronic data have the same legal force that a hand-written signature in written documents has and shall be admissible as evidence in court in all cases, because the client and the bank have mutually agreed over that.[47]

Identification carried out using this method corresponds to the genuine – formal personal identity and this is ensured by institutions issuing electronic certificates and by the banks following the most important principle – proper identification of the client.

3.3. Identification Pursuant to What is a User

In this case biometric identity elements are used which allow identifying a person by specific physiological or behavioural characteristics. Personal characteristics, which can not change, are used and this requires specialised equipment. Most often are used: finger prints, scanning of the eye retina and scanning of the eye iris. Less reliable methods are facial image, hand geometry, recognition of the signature and recognition of the voice. Such technologies have many advantages:[48]

- Biometric characteristics can not be transferred to another individual.
- Biometric techniques prevent errors associated with erroneous assessment resulting from pre-formed opinion, distraction or tiredness.
- One does not need to carry any additional objects (passport, payment card), nor to remember different passwords and codes.

Although this technology is the safest of all that have been discussed, however, its price and complexity of integration makes us chose other, cheaper personal identification measures. In principle, legal acts do not govern this way of identification, except the governing of biometric data stored on identity card.

47 Law on Electronic Signature of the Republic of Lithuania. *Official Gazette*. 2000, No 61-1827, Article 8.

48 Li, S. Z.; Jain, A. K. *Encyclopedia of Biometrics*. Springer Science Business Media, LLC, 2009, p. 2−5.

4. Electronic Personal Identity and Legal Regulation

One of the most important questions relating to the legal regulation of electronic identity is creation of such identity[49]. As has already been mentioned, identity in cyberspace is mostly established by what the user has (confirmed identity), however, over the last several years other identities chosen by a user evolved in cyberspace, which are divided by profiles created in the official environment or in the personal environment.

It is possible to describe in a graphic manner the use of electronic identification methods and measures and the relationship with a real person. Figure 2 provides generalised information concerning measures for the establishment of personal identity both in physical and cyberspace. On the left side of the Figure are shown measures intended to establish personal identity in physical space. On the right side of the Figure are indicated approved measures of electronic identity when a person can be established unambiguously. Meanwhile, at the bottom of the Figure are shown mostly used, non-approved identity measures.

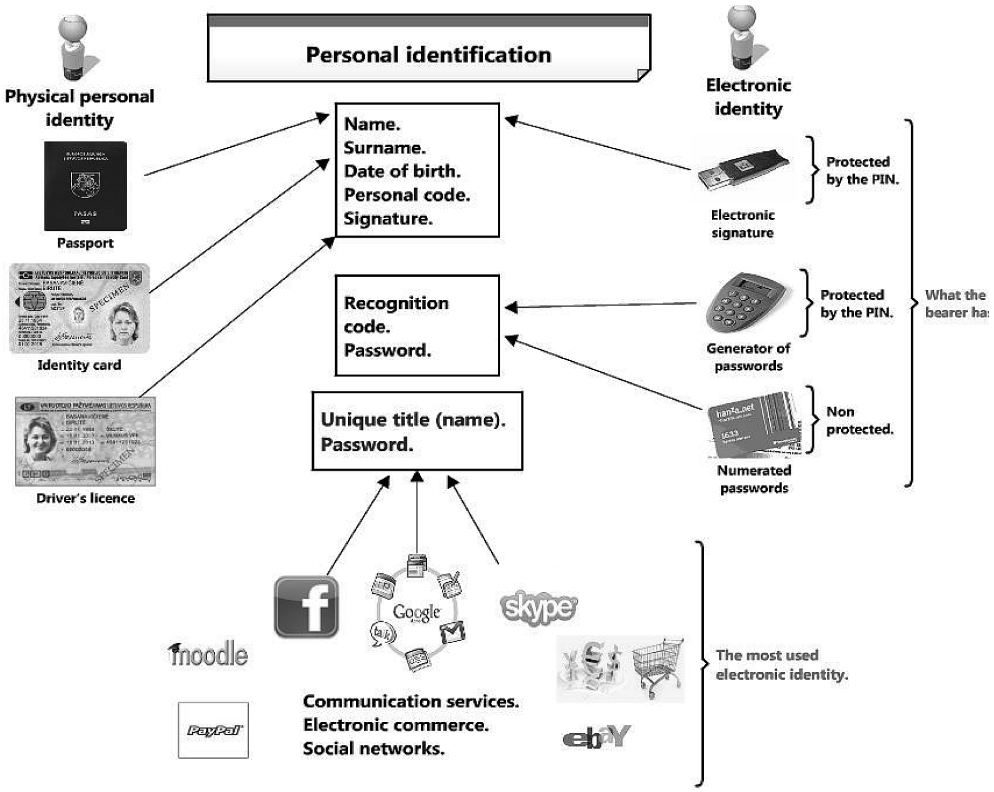


Figure 2. Most recently used electronic identity elements in e-commerce and other e-services, designed by authors.

49 Pirmoji iniciatyva ES šalyse vykdomas projektas STORK (angl. Secure idenTity acrOss boRders linKed), adresas internete <www.eid-stork.eu>.

In case of non-confirmed identity, the process of establishing identity is mostly based on one indicator which is easier falsified and less secure. Cases of identity thefts are most common namely in the systems of this type. In cyberspace identity created by the users themselves is used most of all and it is not difficult to appropriate it.

Identification used in personal environment creates more problems, expands and supplements methods of establishing identity, because users in different systems use versatile ways of establishing identity. In this way, situations are formed when one person has 20, 30 and more measures of electronic identification. These measures of identification are often forgotten, therefore trash of electronic identity is increasing.

A question may arise if it is necessary to guarantee a right to have a correct, not distorted electronic identity. This right covers relatively new legal relationships when a subject reasonably expects that his electronic identity will properly identify him and nobody else will be able to have such identity. This right is closely associated with the idea of the contextual integrity identity, it protects from incorrect identifications. The aspect of the protection of consumers' rights should be also mentioned based on which the state should undertake certain measures to eliminate easily accessible ways of appropriating identity of a respective user (and it is probable that some type of damage can be done to a respective user).

Often emphasized is freedom of choice for users while creating electronic identity, but this sometimes forces selecting cheaper identification systems. Users face numerous identification systems and methods, which connect different elements of identity and apply different standards and technical processes. It is difficult to understand how each system works and it is difficult to use them. It is necessary to address problems of education and consciousness so that users could properly manage their electronic identities. Education is important while creating trust and reducing users' concerns. The key element in increasing privity is accounting and high level of transparency. However, more and more questions arise due to a big number of systems and complexity of the systems; considering this fact, measures should be developed whereby efforts will be made to increase knowledge of citizens and discuss the measures which would require bigger accountability from the suppliers of electronic identity services.

Another question is whether it is possible to instruct obligatorily business to create safe and state-recognized identities. On the one hand, intruding in business is a faulty practice. But on the other hand, a goal of ensuring protection of consumers' rights justifies certain compulsory state instructions.

In the authors' opinion, the most optimal solution would be to allow that market decides which specific measures should be used for identification, but the state must encourage doing this (through the legal regulation). The state should set minimal requirements for identification in cyberspace. It should be indicated which data and elements of identity must be identical in different sectors while identifying a person in cyberspace. An agreement should be reached and appropriate practice taken over from the state, when the same personal data is used for the creation of identity in cyberspace as in physical space.

Authors also propose to foresee within legal norms that, in case of using unreliable identification measures (not recognized by the state), the supplier of the services is made

responsible for[50] consequences caused by illegal actions. Therefore, it is worth while thinking that such regulation would encourage the market start using reliable identification measures (based on what the user has). And then the market, building on the principle of neutrality of technologies, would itself be able to select technology to be used.

It should be also mentioned that there exist certain problems which prevent development of electronic identity. Absence of concepts related to electronic personal identity: full, partial identifier of identity, virtual identity, profiles of the Internet users; at the present time this has not been legally defined. Absence of clear and common concepts distorts treatment, impede to achieve a uniform legal agreement on the question of the said definition. Besides that, different sources of law have no uniform terminology. Necessity of specific definitions evolves due to relationships in cyberspace and their proliferation. Provision of different electronic services requires to establish the parties, their rights and duties, to foresee ways of identifying subjects (name, surname, number, organization and establishment), traceability of such an identifier, authentication of the parties and, apart from that, a subject must know identity of the service provider.

Conclusions

1. Personal identity should be deemed as entirety of data used for personal identification. Regardless of measures and ways of identification both in physical and in cyberspace, there is one personal identity.

2. Physical identity is most often associated with the state-approved identification measure, i.e. with a respective official document issued by the state. The content of information of identification used in respective documents differs depending on the purpose of the document.

3. Measures and ways of identification in physical and cyberspace are not the same. Information identifying persons in physical space and cyberspace may differ by the requirements raised to it. Identification in cyberspace, in particular due to specificity of this space (identification in cyberspace takes place without direct physical presence of the individual), is carried out more often.

4. Identification in cyberspace, using an electronic signature verified with a qualified certificate (as a secure identification measure regulated by the state) or personal identification using banking systems (state-recognized identity[51]) in terms of safe identification conforms to the state-regulated ways of establishing identity in physical space (when identity is established building on the documents).

5. Additional measures and ways of identification are used in cyberspace, which are not legally regulated and thus less secure, resulting in bigger possibilities of identity thefts.

---

50 Obligation to compensate incurred losses.

51 In case of using agreed electronic signature.

6. The state should set minimal requirements for identification in cyberspace. It should indicate which data and identity elements must be identical in different sectors while identifying a person in cyberspace.

7. The state, in accordance with the norms of law, should regulate that, in the case of using insecure identification measures, a responsible businessman must assume solidary liability for the consequences (damage) caused by illegal activity. In this way use of secure identification measures and ways (approved or recognized by the state) would be promoted in business.

References

1 December 2008 Order of the Director of Information Society Development Committee at the Government of the Republic of Lithuania „Rules for the functioning of the interoperability system of information systems of public administration institutions“. No T-228. *Official Gazette*. 2008, No 145-5850.

22 July 2008 Order of the Minister of Justice of the Republic of Lithuania No 1R-294 „On the Amendment of 19 May 2006 Minister of Justice Order No 1R-160 „On the Approval of the Rules of the Civil Registry Office““. *Official Gazette*. 2008, No 88-3541.

A driver's licence is also proposed as a document confirming personal identity [interactive]. 2010-04-30 [accessed 23-03-2011]. <http://www.vrm.lt/index.php?id=131&backPID=1340&pS=1270069200&pL=2591999&arc=1&tt_news=2466&>.

Alcoff, L.; Hames-Carcia, M.; Moya, P. M. L. *Identity Politics Reconsidered*. Palgrave Macmillan, Basingstoke, 2006.

Cane, P.; Conaghan, J. *The New Oxford Companion to Law*. Oxford University Press Inc., 2006.

Civil Code of the Republic of Lithuania. *Official Gazette*. 2000, No 74-2262.

Electronic Authentication Guideline. Recommendations of the National Institute of Standards and Technology. NIST Special Publication 800-63 Version 1.0.2. [interactive]. [accessed 23-03-2011]. <http://www.usda.gov/egov/egov_redesign/intranet/eauth/SP800-63V6.pdf>.

Electronic Authentication Guideline. Recommendations of the National Institute of Standards and Technology. NIST Special Publication 800-63 Version 1.0.2. [interactive]. [accessed 23-03-2011]. <http://www.usda.gov/egov/egov_redesign/intranet/eauth/SP800-63V6.pdf>.

European Council, LTU-FO-02002 [interactive]. [accessed 23-03-2011]. <http://www.consilium.europa.eu/prado/LT/2812/docHome.html>.

First INTERPOL information security conference to provide global platform for preventing and detecting high-tech crimes [interactive]. [accessed 01-12-2010]. <http://www.interpol.int/public/ICPO/PressReleases/PR2010/PR070.asp>.

Google targeted in e-mail scam [interactive]. [accessed 23-03-2011]. <http://news.bbc.co.uk/2/hi/technology/8292928.stm>.

Guide to Authentication Standards for Online Services. State Services Commission, June 2006, Version 1.0. Crown Copyright. [interactive]. [accessed 23-03-2011]. <http://www.e.govt.nz/plone/archive/services/authentication/standards/guide-to-authentication.1.html>.

Higgins, H. E. *Cybercrime: An Introduction to an Emerging Phenomenon*. McGraw-Hill, 2010.

Interpol chief has Face book identity stolen [interactive]. [accessed 23-03-2011]. <http://www.networkworld.com/news/2010/091910-interpol-chief-has-facebook-identity.html>.

Last, J. M. *A Dictionary of Public Health*. Oxford University Press, Inc., 2007.

Law on Cards of Personal Identity of the Republic of Lithuania. *Official Gazette*. 2001, No 97-3417.

Law on Electronic Signature of the Republic of Lithuania. *Official Gazette*. 2000, No 61-1827.

Law on Identity Cards of the Republic of Lithuania. *Official Gazette*. 2001, No 97-3418.

Law on Passport of the Republic of Lithuania. *Official Gazette.* 2001, No 99-3524.

Law on Safe Traffic on Roads of the Republic of Lithuania. *Official Gazette*. 2000, No 92-2883.

Law on the Population Register of the Republic of Lithuania. *Official Gazette*. 1999, No 28-793.

Li, S. Z.; Jain, A. K. *Encyclopaedia of Biometrics*. Springer Science Business Media, LLC, 2009.

Order No 1V-328 „On the approval of rules to issue driver's licence of motor means of transport" issued by the Interior Minister of the Republic of Lithuania on 10 September 2008. *Official Gazette*. 2008, No 106-4060.

Personal identity card [interactive]. [accessed 23-03-2011]. <http://www.pasienis.lt/lit/asmens_tapatybės _korteliu_galiojimas_ir_/132>.

Vocabulary of the Lithuanian Language. Vilnius: Institute of the Lithuanian Language, 2005.

ASMENS IDENTIFIKAVIMO FIZINĖJE IR ELEKTRONINĖJE ERDVĖJE TEISINIO REGULIAVIMO PRIELAIDOS

Darius Štitilis, Paulius Pakutinskas, Inga Dauparaitė, Marius Laurinaitis

Mykolo Romerio universitetas, Lietuva

Santrauka. *Straipsnyje nagrinėjamos asmens identifikavimo fizinėje ir elektroninėje erdvėje teisinės prielaidos. Analizuojamas teisinis identifikavimo fizinėje ir elektroninėje erdvėje reglamentavimas. Pateikiami privalomi identifikavimo fizinėje erdvėje elementai bei privalomi ir neprivalomi identifikavimo elektroninėje erdvėje elementai ir daromos išvados dėl asmens identifikavimo elektroninėje erdvėje probleminių aspektų ir su jais susijusio teisinio reguliavimo.*

Mokslinį straipsnį sudaro keturi pagrindiniai skyriai. Pirmame skyriuje „Tapatybė ir asmens identifikavimas" nagrinėjama tapatybė, jos turinys ir elementai bei asmens identifikavimas. Antrame skyriuje „Asmens identifikavimas fizinėje erdvėje" išsamiai analizuojamos identifikavimo fizinėje erdvėje teisinės prielaidos Lietuvoje. Trečiajame skyriuje „Asmens identifikavimas elektroninėje erdvėje" analizuojami teisiškai sureguliuoto ir nesureguliuoto asmens identifikavimo elektroninėje erdvėje elementai, aptariama asmens tapatybė elektroninėje erdvėje. Ketvirtame skyriuje „Elektroninė asmens tapatybė ir teisinis reguliavimas" analizuojami ir sisteminami elektroninės asmens tapatybės elementai, ir daromos prielaidos dėl jų patikimumo bei teisinio reguliavimo privalomumo.

Atlikus analizę ir atitinkamus tyrimus, prieita prie pagrindinių išvadų, jog identifikavimo priemonės bei būdai fizinėje ir elektroninėje erdvėje nėra tie patys. Asmenis identifikuojanti informacija fizinėje ir elektroninėje erdvėje gali skirtis pagal jai keliamus reikalavimus. Elektroninėje erdvėje naudojamos papildomos identifikavimo priemonės ir

taikomi būdai, kurie teisiškai yra nereguliuojami ir dėl to mažiau saugūs, sudaro didesnes galimybes padaryti tapatybės vagystę. Dėl šių priežasčių valstybė turėtų nustatyti minimalius identifikavimo elektroninėje erdvėje reikalavimus.

Reikšminiai žodžiai: *asmens identifikavimas, tapatybė, fizinė erdvė, elektroninė erdvė.*

Darius Štitilis, Mykolo Romerio universiteto Socialinės informatikos fakulteto Elektroninio verslo katedros docentas. Mokslinių tyrimų kryptys: elektroninė komercija, elektroniniai nusikaltimai, asmens duomenų teisinė apsauga.

Darius Štitilis, Mykolas Romeris University, Faculty of Social Informatics, Department of Electronic Business, associate professor. Research interests: electronic commerce, cybercrime, personal data protection.

Paulius Pakutinskas, Mykolo Romerio universiteto Mokslo centro mokslo darbuotojas, socialinių mokslų daktaras (teisė). Mokslinių tyrimų kryptys: elektroninių ryšių teisė, interneto teisė, IT teisė.

Paulius Pakutinskas, Mykolas Romeris University Research Center, researher, doctor of social sciences (law). Research interests: electronic communications law, internet law, IT law.

Inga Dauparaitė, Mykolo Romerio universiteto Mokslo centro jaunesnioji mokslo darbuotoja. Mokslinių tyrimų kryptis: IT teisė.

Inga Dauparaitė, Mykolas Romeris University Research Center, junior researcher. Research interest: IT law.

Marius Laurinaitis, Mykolo Romerio universiteto Ekonomikos ir finansų valdymo fakulteto Bankininkystės ir investicijų katedros lektorius. Mokslinių tyrimų kryptys: elektroninės mokėjimų sistemos, elektronianai pinigai, mobilūs atsiskaitymai, pinigų plovimo prevencija.

Marius Laurinaitis, Mykolas Romeris University, Faculty of Economics and Finance Management, Department of Banking and Investments, lecturer. Research interests: electronic payment system, e-money, mobile payment, money laundering prevention.