DOI: 10.2507/29th.daaam.proceedings.069

TECHNOLOGICAL AND LEGAL ISSUES OF IDENTIFYING A PERSON ON THE INTERNET TO ENSURE INFORMATION SECURITY

Anna Zharova[a,b], Vladimir Elin[a] & Peter Panfilov[a]

[a]*National Research University – Higher School of Economics, Myasnitskaya St. 20, Moscow 101000, Russian Federation*
[b]*The Institute of State and Law of The Russian Academy of Sciences, Znamenka St. 10, Moscow 119019, Russian Federation*

This Publication has to be referred as: Zharova, A[nna]; Elin, V[ladimir] & Panfilov, P[eter] (2018). Technological and Legal Issues of Identifying a Person on the Internet to Ensure Information Security, Proceedings of the 29th DAAAM International Symposium, pp.0471-0478, B. Katalinic (Ed.), Published by DAAAM International, ISBN 978-3-902734-20-4, ISSN 1726-9679, Vienna, Austria
DOI: 10.2507/29th.daaam.proceedings.069

Abstract

This article investigates the problem of identifying a person on the Internet by legal and technical means. The practice of identifying people in Russia and the UK was studied and compared. Russia was selected because its legislation is well known to the authors, and the UK was selected as it has developed a mature system for the online identification of individuals and relationships and a certain legal regulation in this sphere. An analysis of two government programs was made, namely: the UK Identity Assurance Programme of the Government Digital Service and the Russian Government Decree on "The development of the Federal state information system". In terms of technological background for person's identification, the practice of using IPv4 and IPv6 was explored. Russia's specific problems are analysed via the protection of privacy in the case of personal identification and the processing of personal data on the Internet. The authors draw conclusions about the division of the concepts of identification and individualization of people on the Internet. We introduce our own definition of personal identification on the Internet and propose an amendment to the Russian concept of personal data: the definition of personal data should include the IP address of a person.

Keywords: personal identification; IPv4; IPv6; anonymity; privacy protection

1. Introduction

The spread of information technology allows the creation of false personal data on the Internet and the abuse of opportunities, which leads to the emergence of anonymous individuals and anonymous relationships. Anonymity is solved many countries through the implementation of procedures to identify a person on the Internet. The question of personal identification is particularly acute in cases of the provision of public services and the legal resolution of illegal activity on the Internet. The reason is that the anonymous user does not have the nominative attributes typical for a person in the offline environment and by which the other participants of online relationships can be assured that the actions carried out are by a particular person. There is the substitution of one person by another, who may not exist in the (offline) world.

This person is a virtual entity who undertakes action having legally significant consequences, for example, the person can make purchases or disseminate information [1]. Reza Etemad-Sajadi and Lassaad Ghachem [2] examine in detail the actions of online avatars. Transactions are concluded by non-existent persons. This anonymous person "lives" only on the Internet but this person is a real offline person who is immersed in the Internet using false personal data. From the point of view of law, this virtual person should be seen as inauthentic and his activity should be seen as a simulation. In terms of legal classification the actions committed by a virtual person should be considered wrongful.

The problem is collecting and processing real personal data on the Internet, because the legal identification of a person is possible only by personal data [3]. This situation will exist until legislation understands personal data only as real data [4].

Of course, the collection of personal information is related to the principle of non-interference in the privacy of a person. It is necessary to strike a balance between privacy protection and the interests of other participants in online relationships. Most countries require the consent of the person for the collection of personal information. However, there are situations in which a person refuses to provide this information voluntarily or the data does not correspond to reality. Most countries believe there is a need to develop the regulatory and technological requirements for activities carried out on the Internet. "Today, security has become a top priority subject on many countries' agendas, as governments find themselves faced with continuous radical strategic challenges related to identity management and verification". Two questions arise:

What are the administrative and technological regulations for obtaining data which must be developed on a country level?

What is the legal framework in these relationships?

It should be understood that we cannot solve these problems only by legal norms. We can eliminate the existing legal uncertainty only by combining legal and technical/technological methods of individual identification. The rest of the paper is organized as follows. In the beginning, Section 2 introduces personal identification problem on the Internet and existing legal and technical solutions that should allow people to be identified while providing adequate information security. In Section 3, problems of personal identification in Russian landscape are discussed in details. It presents issues of a legal identification of a person based on differences in the legal regulation of relationships in the virtual and in the real environment system. Also a personal identification by technical means in legal acts is discussed. Then, in Section 4, the systems of identity confirmation for the provision of public services in the UK and Russia are discussed and compared that comprises certain procedures, municipal services and technical means or tools to assure identity. Finally, section 5 summarizes the research findings and suggests some future developments.

2. The issue of personal identification on the Internet

In Russia, to resolve the problems of personal identification on the Internet and for the development of legislative proposals, the basic research and strategic objectives were identified. The Office of the President of the Russian Federation identifies the following areas of research in the field of information security on the Internet: the development of “a state system of trust management for information to ensure the protection of personal data and cross-border transfers; the development of Internet content and increased confidence in the Internet; the development of methods to qualify the hostile use of information and communication technologies and models of an inter-state system of monitoring threats to international information security” [5].

The Concept of the Convention “On ensuring international information security in the Russian Federation” refers to "uncertainty in identifying the source of hostile action, especially in view of the increasing activity of individuals, groups and organizations, including criminal organizations which carry out mediation of on behalf of others" (The Concept of Convention on ensuring international information security) [6].

The main requirement of Russian law on the right of personal data processing is the obligation to obtain consent from the individual. Unfortunately, in Russia there is no unified technological system of interaction between state structures which could provide data interchange at the request of one of the services. Currently, for each service, the state structure or the organization should themselves receive personal data from the individual. If the consent of the person was not received by the organization, then the organization is not entitled to handle such data. This gives rise to the strange situation where for example, the rescue service “112” is called. They ask the person about his location and offer to call to the others emergency services. Thus, in Russia the problem of identification person is quite acute.

Roscini [7] writes on problem of identification, “[it] presents significant technological problems. Anonymity is in fact one of the greatest advantages of cyberspace… Nonetheless, the challenges in the identification of attackers should not be an excuse not to tackle the international legal aspects of cyber operations. After all, identifying the authors of hostile actions is a problem also in other contexts, for instance international terrorism”.

The website of the US Department of Justice says that “identity theft and identity fraud are terms used to refer to all types of crime in which someone wrongfully obtains and uses another person's personal data in some way that involves fraud or deception” (US Department of Justice). In cases of the illegal use of other people's data, the US Department of Justice specifies obtaining economic benefits [8]. However, cases of non-economic relationships raise the question of the use of false personal data.

Moreover, the data which confirm the identity of the person on the Internet needs to be identified. Is it being a violation if, by coincidence, we have the same (nick)name as another person?

Identification and privacy are inextricably linked. In many countries, the concept has been fused with data protection, which interprets privacy in terms of the management of personal information. Russian legislation interprets privacy in terms of the management of personal information [9]. Para. 1. of Decree No 188 defines personal data as "information about the facts, events and circumstances of the private life of a citizen, which allows the person to be identified, except the information that is disseminated in the mass media in the cases established by federal laws." The Russian Constitution protects privacy and it attributes to privacy both family secrets and personal secrets (art. 23). I consider absolutely correct the separation of privacy at different levels, each of which should be determined by specific criteria. Stelios Dritsas, Dimitris Gritzalis and Costas Lambrinoudakis [10] offer the following four-part classification of privacy: "Territorial privacy: the protection of the physical area surrounding a person. Bodily privacy: the physical protection of a person against undue interference. Informational privacy: the awareness and control of whether and how personal data can be gathered, stored, processed and communicated. Privacy of communications: the protection of data communicated among persons, which prevents the monitoring of the transmitted data by third parties".

In order to ensure information security both technological and legal requirements for personal identification on the Internet must be provided. For example, Ayoade John and Kosuge Toshio [11] propose the establishment of the Solution to Privacy and Lawful Access Conflict (SPLC). "This process will allow users their privacy by using security techniques that meet their needs, but users will need to notify the SPLC about the transmission of the secret information".

Such technology will disadvantage people. However, in order to ensure information security for other people both the technological and legal requirements should allow people to be identified. Therefore, we must decide what guarantees that the person on the screen is a real person. Kevin Aquilina [12] writes "computer systems should be created with the idea of developing computer security and privacy, both with regard to hardware and software, so that they are designed with security and privacy in mind. Privacy should not be considered as a side effect in the development of new technologies incorporating security features. In this way technology is developed right from the beginning as being security and privacy compliant and the industry would not need, at a later stage, to develop privacy enhancing technologies to fill in the gap by redesigning the already existing privacy intrusive technology" [12].

3. Problems of personal identification

3.1. The legal identification of a person in accordance with Russian legislation

Let us consider the differences in the legal regulation of relationships in the virtual and in the real environment. In criminal law, anonymity is prohibited. In criminal proceedings there is a mandatory procedure of establishing a person's identity. The exception is for the protection of witnesses, but in this procedure anonymity is limited because the witness is unknown to the participants of the process but not to government officials. The Russian Civil Code defines the possibility of the individualization of the citizen by name, which includes the surname, first name and patronymic if this is required by law or national custom. However, the Civil Code provides limited cases for the use of a pseudonym. For example, there are legal procedures in which a person may be anonymous: the right of an author to use a pseudonym or publish the result of intellectual activity without his name (art. 1265 Civil Code); the right of a person to change his name (para. 1 and 2 of art. 19 of the Civil Code) and the right of a blogger to use his name or a nickname for expressing personal judgments and evaluations on their site or page on the Internet (art. 10.2 Federal Law "On Information").

The Civil Code defines that a citizen cannot acquire rights and duties for himself under the name of another person, but he can act on behalf of another citizen as his representative in accordance with the contract or law for the emergence of the legal effects on the side of the submitter (para. 1, para. 1, Art. 28, para. 2, Art. 29, para. 1, para. 1, Art. 182, para. 1, Art. 971, para. 3 para. 1 of Art. 1005 of the Civil Code).

There a clear difference between an individual acting on behalf of another person in accordance with a contract, and an individual acting on behalf of a non-existent person. For example, in November 2015 in Japan, a man was arrested who visited Facebook 18 times under assumed names [13]. There are examples of actions undertaken on the Internet using false personal information. These are described in the article by Reza Etemad-Sajadi and Lassaad Ghachem [2]. They state that "the avatar can (1) welcome users to the website, (2) assist the users to browse the website, (3) answer users' questions, (4) simulate a real-time conversation, (5) have several parallel conversations, (6) reduce costs for the company through acting in lieu of a customer service operator, (7) collect data on users and their needs, (8) reinforce the company's brand, (9) create an enjoyable or 'fun' experience for users, (10) manage relationships with current and potential clients, (11) increase users' desire to visit the company, and finally (12) create a positive experience that can be passed on by word of mouth. Despite very optimistic literatures, the virtual agents do not seem to always live up to all their promise" [2].

A person who enters into relationships on the Internet can easily hide the name which has been determined by the legislation. The only way to identify him is the IP-address by which a person joined the network. Some countries have implemented the requirement to identify a person by attaching a copy of his passport at the time of registration on a site. However, this method of identification does not solve problem, for creating a fake copy of a passport is technologically easy.

If the platform for the organization of personal relationships is ICT-based, then the method of identifying person uses other techniques to determine the entry point of the person on the network and can correlate this fact with previous information [14] such as information about the IP-address or of the provider by which a person has joined the Internet.

3.2. Identification by technological methods in legal Act

The Declaration of Principles Building the Information Society states, "A global challenge in the new Millennium indicates the need to use the next-generation IPv6 by which the citizens can gain easier access to government services" (Declaration of Principles Building) [15]. For this purpose, the Declaration calls to unite the efforts of the member states to create a single information space.

According to 2013 information, only 3% of the population are using the updated IPv6 protocol (IPv6 in 2013). "IPv6 traffic on the Internet is still in 2015 only app. 4% of total traffic[….] Even though, there has been a considerable growth in the adoption of IPv6 in the past three years, from less than 1% in 2012 to 4% in 2015" [16, 17].

Another side of the use of IPv6, relates to information security. Marco Roscini writes "further developments in computer technology and internet regulations, such as the introduction of the new internet protocol IPv6, might also make identification easier" [7]. However, network users can create anonymity on different levels. Firstly, this opportunity is created by the developers of the site at where information is exchanged [18]. Secondly, the participants can create an anonymous presence on the Internet using, for example, the tor-network.

These levels differ by the possibility of finding the IP-address with which a person violates the law. In the first situation, with the presence of a number of legal, organizational and technical requirements, the network provider can identify the IP-address. In the second case, the participant creates a situation in which a provider cannot determine the IP-address or it is too difficult and expensive. It should be taken into account that technology is constantly evolving and new mechanisms for the creation of anonymity on the Internet constantly arise. Although there is the meaning that "technological privacy enhancement mechanisms are not catching up" [12].

Technology creates such opportunities for relationships must be regulated by technology on the Internet [19]. For example, the authentication method of information technology is used in "Identity Management". In the description of this technology it is specified that "technological digital identity is carried over individuals, group of individuals or entities, the software, any device that can request the use of a resource of the Internet. In turn, the resource can be a Web-site, a piece of data in the database, the transaction by a credit card and so on" [20].

Despite advanced technology, in Russia access to the Internet public access remained problematic before 2014. In Russia, August 18, 2014, the Government Resolution on the prohibition of anonymous entry via Wi-Fi zone was signed. In addition, Russia introduced technology to pre-filter sites and pages of sites for harmful information. This pre-filtration is conducted on two levels: by lists of banned sites placed on the Federal Service for the Supervision of Communications, Information Technology, and Mass Media (Roskomnadzor), and a system of recognition of harmful information. Recognition of harmful information can be possible only for the following categories of information such as suicide, drugs and child pornography. In 2013, the Russian Federation adopted an Order on behalf of the three executive authorities with competence in this field (these are the Federal Service for the Supervision of Communications, Information Technology, and Mass Media; the Federal Service for Drug Control of Russia and the Federal Service for Supervision in the Sphere Consumer Rights Protection and Human Welfare) which determines harmful information by the criteria determined in this Order [21].

To solve the problem of identification, the scientists proposed to use a certified Internet technology. Lawrence Lessig writes that "certification in cyberspace could be much more narrowly tailored. If a site required that only adults enter, you could—using certification technologies—certify that you were an adult, without also revealing who you were or where you came from. The technology could make it possible to selectively certify facts about you, while withholding other facts about you. The technology could function under a "least-revealing-means" test in cyberspace even if it cannot in real space" [22]. It should be borne in mind that each country determines independently the degree of harmfulness of information, and in this regard, common regulatory rules are impossible to develop. As a solution, we propose the mandatory implementation of the principle of interoperability. This principle allows the preservation of the uniqueness of each information technology, and facilitating the integration of one technology with another, including technologies of different states [23].

We conclude that the absence of developed technological procedures which allow any person to accept or to reject identification leads to "legal fiction". Dritsas S. et. al. [10], described the need of such technological procedures. The essence of the phenomenon is that a non-existing fact is recognized as existing, or vice versa. A fictitious, anonymous person exists only in a virtual environment and is absent in the real world. Such non-existing people enter into legal relationships. For government relations, identification should be a mandatory procedure. Let us consider which actions are taken by states to create a network of trusted relationships on the Internet.

4. The systems of identity confirmation for the provision of public services: Examples of the UK and of the RF

The need for the reliable, fast and secure identification of people and their actions on the Internet has been recognized in the UK and Russia (and elsewhere) as a key factor in the successful use of the Internet.

Those responsible for the provision of public and social services are in a position where the disregard of safety and the necessity to identify and authenticate can have serious financial and administrative implications. “The Identity Assurance Programme” has operated in the UK since 2014. The program is a key element of the reforms implemented in digital services. It focuses on the development of systems to ensure the online identity of the person in the UK, in order that citizens, businesses and public authorities are able to safely and securely use information online. For these purposes, a system of identification and authentication has been implemented, the tasks of which are reducing the burden of the management of user data and the creation of a confidential information environment.

The system Electronic Government State Service (Government service) operates in the Russian Federation. The basis of the functioning of this service is the Government Decree on “The development of the Federal state information system”, a unified system of identification and authentication providing information and technological interaction between information systems for the provision of public and municipal services in electronic form [24]. The Unified system must provide personal registration and identification. This allows users to get different government services.

Registration is carried out using passport and insurance data. In this case a person can get state services which do not require a physical human identification. Registration in the unified system can be implemented by simple electronic signatures or qualified electronic signatures (e-signatures) [25]. To obtain a passport requires additional steps of confirming the identity, requiring a person to obtain an activation code at the Russian postal service (or an organization which will give a code which can also be sent to a mobile phone). However, a mobile number is given by the passport data only, so in this case the person has been physically identified.

The unified system can require the use of a qualified electronic signature for certain purposes. These actions also complicate the use of this system. A qualified electronic signature is the most difficult to obtain. This signature cannot be formed by the users themselves it should be obtained from the Certification Authority issuing e-signatures.

In addition, the use of qualified e-signatures initially should be agreed on between the participants of relationships. In accordance with the Federal Law "On electronic signatures" [25], the use of this signature eliminates issues of human identification. However, despite its versatility, getting such a signature is expensive and requires a physical presence at the Certification Authority. To summarize in Russia to receive public services online a person requires physical identification.

The procedure of identification and authentication in the unified system is founded on a comparison between the participant identification data (ID) or the ID of its information system which are introduced by the participant in the system and information about a participant or its information system that is in the Government basic information registry. The ID of the information system or of the individual is a unique sequence of characters, the use of which accesses information contained in the Government information registry.

The main drawback of the unified system is the narrow focus associated with the provision of public and municipal services in electronic form. The system cannot be used for the detection of persons who have committed offences in the Internet. Figure 1 gives the scheme for the provision of public services in Russia [26].

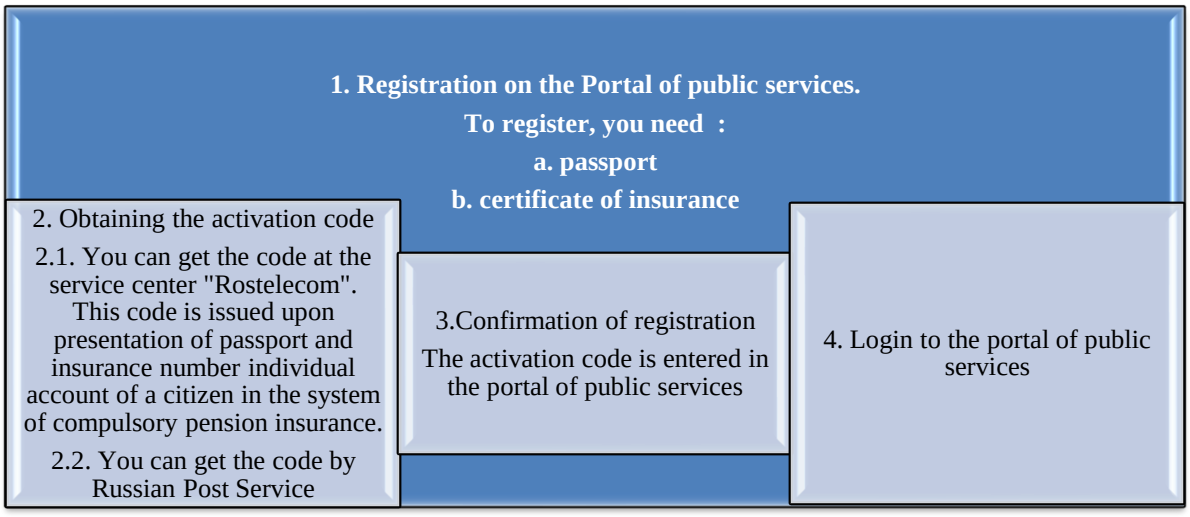

Fig.1. Steps to accessing a secure government service of Russia

For comparison, Figure 2 gives the scheme for the UK [27]. The “Identity Assurance Programme” specifies that “identity assurance is only required for secure transactions or personal information. The individual chooses the identity provider. This is a federated approach to identity assurance. There are currently 5 identity providers. The individual gives the identity provider information for registration. The identity provider reviews the evidence to confirm the identity. The identity provider gives the individual log-in details. The identity provider systems confirm the identity and notify departmental services. Departments match the individual’s identity with their service records. The individual signs in securely with their identity provider to access digital services” [28].

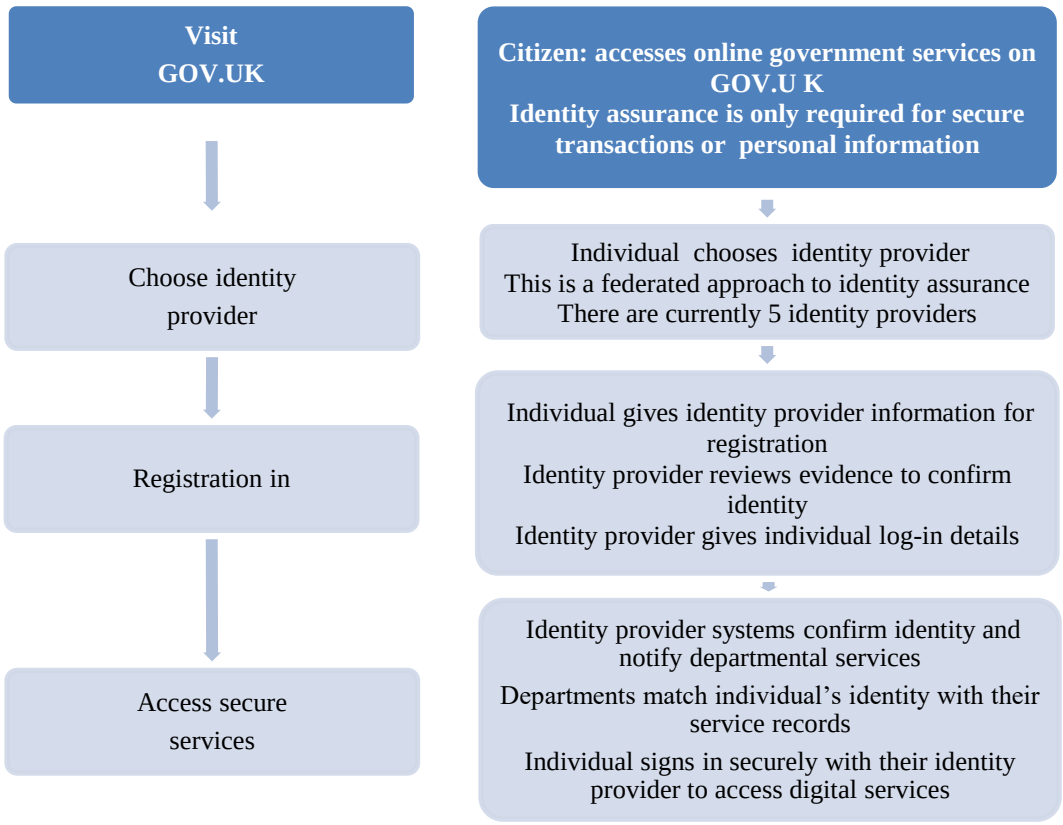

Fig. 2. Steps to accessing a secure government service of UK.

4.1. Comparing systems

Comparing these schemes, providing services in the Russian Federation is only possible after a person's identity is confirmed by a public authority. To get a qualified signature, the physical verification of the person who has been issued the signature is required [29].

In the UK identification is done by identity providers. "Through a standards based approach, contracted and certified private sector organisations (identity providers) enable citizens to use evidence they own as part of the process for validating and verifying their identity" (Identity assurance: delivering trusted transactions).

The UK system is a more mobile system, not directly linked to a public authority. The partnerships between identity providers allow the use of this system in the majority of Internet relationships. The Russian identification system does not provide for the expansion of the number of Internet relationships, i.e. outside government services.

In the UK, standards of identification and authentication on the Internet have been jointly developed, agreed on and certified by the public and the private sector. This allows identity providers to provide services of good quality, and users have greater guarantees in the commission of such operations. In one day, the identity provider has identified the person and established relationships with the user; it has the rights and obligations to verify the user's identity in specified situations or at the request of the user.

In Russia, there are no generally accepted standards of identification and authentication for the verification of a person on the Internet. Currently, the private sector itself solves this problem of lack of a unified trusted space on the Internet. For example, Russian banks are developing their own identification system to ensure the identity of the bank customer. At present in Russia the reliable online identification of the person is possible only when using a qualified electronic signature (art. 5 Federal law "On electronic signature"). All other cases use a simple electronic signature, IP-addresses, a domain name, username and password and can be recognized false [3].

5. Conclusion

To determine the relevance of the issue of information security through the identification of a person as a participant of the online relationships a review of the literature was carried out, which points to the need to address the problems identified. The article draws a parallel between the regulations and the opinions of technical specialists, who point out the problems of implementing the regulations. The research methodology is based on an analysis of Russia legislation, the literature review, and an analysis and observations of research articles that were accessible between 2000 and 2018.

An analysis of two government programs was made—the UK Identity Assurance Programme of the Government Digital Service; and the Russian Government Decree on "The development of the Federal state information system". The latter is a unified system of identification and authentication providing information and technological interaction between information systems which are used for the provision of public and municipal services in electronic form. The analysis showed different approaches to the identification of a person both at the level of technological development and at the level of the organizational and legal regulation.

In Russia, the concepts of the identification and individualization of a person are divided. Identification is the process of confirming a person by both technological and regulatory procedures on the Internet. Individualization is the detection of true personal data of the person which is based on legal norms. Thus the Russian experience shows that personal data must include an IP address and other identification data.

The identification of a person is an essential factor to ensure information security. However, it is necessary to strike a balance between the freedoms of individuals on the Internet; their rights should not be violated. There is a need to develop legal rules and the technical regulations which enable the identification of a person if a person undertakes legally significant actions. It is important to develop a system of standards for identification.

6. Acknowledgments

We thank the Russian Humanitarian Science Foundation for their assistance in the project "Comparative legal research methods of information security in the Russian Federation and EU Members (№ 16-03-00679)".

7. References

[1] Zharova, A.K., Elin, V. (2017). The use of Big Data: A Russian perspective of personal data security. Computer Law & Security Review. 2017. Vol. 33. No. 4., pp. 482-501

[2] Etemad-Sajadi R., Ghachem L. (2015). The impact of hedonic and utilitarian value of online avatars on e-service quality. Computers in Human Behavior 52, pp. 81–86.

[3] Zharova A.K., Elin V., Panfilov, P. (2017). PERSONAL DATA IN CLOUD. RUSSIA EXPERIENCE. Some features of the legal regulations on the use of personal data in cloud technologies using the example Russian legislation, in: 28 TH DAAAM International Symposium on Intelligent Manufacturing and Automation. Wien: DAAAM International Vienna, 2017, pp.1136-1142.

[4] The system GARANT Legislation with comments (2006). Federal law of the Russian Federation on 27 July 2006, in N 149-FZ "On Information, Informational Technologies and Protection of Information". Federal law of the Russian Federation on 27 July 2006, in N 152-FZ, "On Personal Data".

[5] The research work (2015), "Preparation of proposals to improve the protection of personal data." Decree of the Administration of President Russia Federation, March 18, 2015 No 280.

[6] http://csef.ru/en/nauka-i-obshchestvo/445/mezhdunarodnoe-sotrudnichestvo-rossii-v-oblasti-obespecheniya-informaczionnoj-bezopasnosti-5920 (2014), Concept of Convention on ensuring international information security. The site of Security Council of the Russian Federation, Accessed on: 2017-10-12

[7] Roscini, M. (2014). Cyber Operations and the Use of Force in International Law. Oxford University Press, 2016, 307 pages. Print publication date: 2014. Published to Oxford Scholarship Online: April 2014. Print ISBN-13: 9780199655014

[8] http://www.justice.gov/criminal-fraud/identity-theft/identity-theft-and-identity-fraud (2016), United States. Department of Justice. "What Are Identity Theft and Identity Fraud?", Accessed on: 2016-01-13

[9] The system GARANT Legislation with comments (1997), The Presidential Decree "The list of confidential information", March 6, 1997, No. 188.

[10] Dritsas, S., Gritzalis, D., Lambrinoudakis, C. (2006). Protecting privacy and anonymity in pervasive computing: trends and perspectives. Telematics and Informatics. 23, 196–210.

[11] Ayoade, J.O., Kosuge, T. (2002). Solution to Privacy and Lawful access Conflict (SPLC). Telematics and Informatics 19, 273–289.

[12] Aquilina, K. (2010). Public security versus privacy in technology law: A balancing act? Computer Law & Security Review, Vol. 26, No. 2.

[13] http://tass.ru/proisshestviya/2421620 (2015), The Japanese will have been given three years for illegal access to another account in the Facebook site. The news agency in Russia, Accessed on: 2017-10-12

[14] Zharova A. (2015) Influence of the principle of interoperability on legal regulation. International Journal of Law and Management. - Vol. 58, issue: 2.

[15] http://www.itu.int/net/wsis/docs/geneva/official/dop.html (2003, 2005), Declaration of Principles Building the Information Society: a global challenge in the new Millennium, Accessed on: 2017-10-12

[16] Tadayoni, R., Henten, A. (2016). From IPv4 to IPv6: Lost in translation? Telematics and Informatics. 33,650–659.

[17] http://www.internetnews.com/infra/ipv6-in-2013-where-are-we-now.html (2013), IPv6 in 2013: Where Are We Now?, Accessed on: 2017-10-12

[18] Filaretov, V, Zhirabok, A, Zuev, A, & Protsenko, A. (2016). Method of Fault Identification in Mechatronic Systems, Proceedings of the 27th DAAAM International Symposium, pp.0312-0318, B. Katalinic (Ed.), Published

by DAAAM International, ISBN 978-3-902734-08-2, ISSN 1726-9679, Vienna, Austria DOI: 10.2507/27th.daaam.proceedings.046

[19] Elin, V., Zharova, A.K. (2017). Protection of Confidential Information in Educational Information Environments, in: Strategic Innovative Marketing. 4th IC-SIM, Mykonos, Greece 2015. Switzerland: Springer, 2017. Ch. IX. pp. 623-628.

[20] http://citforum.ru/internet/webservice/oracle_app_server/ (2005), Oracle Application Server 10g Release 2. Overview of new features, Accessed on: 2017-10-12

[21] The system GARANT Legislation with comments (2013). Order of Federal Service for Supervision of Communications, Information Technology and Mass Media, No 1022 and the Federal Service of the Russian Federation for Narcotics Control, No 368 and Federal Service for Supervision of Consumer Rights Protection and Human Welfare, No 666, Sept. 11, 2013 "On approval of the criteria for evaluating materials and (or) the information are necessary for decision-making these federal executive authorities about the inclusion of the domain name and (or) indicators site into an automated information system "Unified Register of domain names, indexed pages of Internet sites and the network addresses which enable the identification of sites in Internet that contained the information the dissemination of which is prohibited in the Russian Federation"

[22] Lawrence, L. (2000). Code Is Law. On Liberty in Cyberspace, http://harvardmagazine.com/2000/01/code-is-law-html, Accessed on: 2017-10-12

[23] Husnjak, S., Perakovic, D., Forenbacher, I. & Jovovic, I.: Identification and Prediction of User Behavior Depending on the Context of the Use of Smart Mobile Devices DOI:10.2507/26th.daaam.proceedings.

[24] The system GARANT Legislation with comments (2013). The Government Decree of 10.07.2013 N 584 "On the development of Federal state information system "Unified system of identification and authentication in the infrastructure is providing information and technological interaction between information systems which have being used for the provision of public and municipal services in electronic form "".

[25] The system GARANT Legislation with comments (2011). Federal law of the Russian Federation on 6 April 2011, N 63-FZ, "On Electronic Signature".

[26] http://www.penzgtu.ru/fileadmin/filemounts/maindoc/gosuslugi/gosuslugi_reg.pdf (2017), Step by step instructions. Registration portal of public services, Accessed on: 2017-10-12

[27] http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32014R0910&from=EN (2014), Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC, Accessed on: 2017-10-12

[28] https://www.gov.uk/government/collections/identity-assurance-enabling-trusted-transactions (2012), Identity assurance: delivering trusted transactions (Guidance on identity assurance for government departments and service providers), Accessed on: 2017-10-12

[29] http://www.penzgtu.ru/fileadmin/filemounts/maindoc/gosuslugi/gosuslugi_reg.pdf (2016), The registration procedure of Russia, Accessed on: 2016-01-13