IDENTIFICATION DATA MANAGEMENT: LEGAL REGULATION AND CLASSIFICATION

Oleksii Kostenko
Ph.D., Head of the Research Laboratory of Theory and Law of Digital Transformations
of the Research Center for Digital Transformations and Law
of the Research Institute of Informatics and Law
of the National Academy of Legal Sciences of Ukraine, Ukraine
e-mail: antizuk@gmail.com, orcid.org/0000-0002-2131-0281

Summary

The scale, speed and multi-vector development of science and technology are extremely effective in influencing legal, economic, political, spiritual, professional and other social relations. The development of information and communication technologies, the use of the Internet, the creation, storage, transmission, processing and management of information became the driving forces of the new scientific and technological revolution.

This facilitates the introduction of technologies for the transmission and use of information in digital form in almost all spheres of public life, namely text data, photo, audio, video images, which are transmitted in various ways via the Internet and other systems and means of communication.

One of the key elements of data transmission technologies and systems is the availability of information by which it is possible to identify their subjects and objects by their inherent identification attributes. In Ukrainian legislation, in particular in the Law of Ukraine «On Personal Data Protection», information or a set of information about an individual who is or can be identified specifically is defined as personal data. However, despite its modernity, this law still contains a number of shortcomings and uncertainties, both in terminology and in the legal mechanisms for working with data by which a person can be identified, i.e. identification data.

Keywords: IoT devices, identification systems, identification data management, identification, identification data, technical standards, artificial intelligence, electronic trust services.

DOI https://doi.org/10.23856/4325

1. Introduction

At this stage of development of public relations, the issues of solving the problem of protection of identification data are highly sought. At the same time, the issue of creating a unified identification system with transparent and effective technical and legal rules for the management of identification data has not been comprehensively considered and is currently extremely relevant.

The article is aimed at the development of proposals and recommendations for the creation of a unified classifier of identification data, criteria and mechanisms for their application, the formation of new definitions for the development of conceptual and categorical apparatus in the field of identification data management (identity management, IDM) and improvement of existing ones.

Theoretical and methodological basis of the article are scientific developments of domestic and foreign scientists on current issues in the fields of information and law, which are mostly devoted to regulating the use of personal data, Internet of Things, information security management systems, artificial intelligence, electronic trust services.

Among the domestic works are: A. Anisimov, I. Aristova, O. Baranov, Y. Baturyn, I. Bachylo, K. Belyakov, V. Bryzhko, N. Hrytsyak, I. Gorbenko, V. Pylypchuk, O. Radutny, A. Semenchenko, Y. Tikhomirova.

Research on legal issues of implementation and use of digital technologies in the field of identification data management and their legal regulation is carried out by researchers from different countries, but both the formulation of legal problems and ways to solve them are still at an early stage. In particular, similar research in the field of regulation of identity management is carried out by such scientists as: S. Bouzefrane, K. Cameron, K. Tracy, M. Hansen, E. Kosta, Simone Fischer-Hübner, Elias Pimenidis, J. Loo, M. Aiash, C. Thompson, A. Cavoukian.

The works of these and many other authors, of course, have scientific and practical significance, but they do not give a holistic view of the modern unified system of identity management. Among Ukrainian scientific organizations, the issues of the proposed research have not been explored before, and Ukrainian scientists have not yet published the results of such research.

2. Problems of identity management

Modern society has entered the stage of scientific and technological revolution 4.0, economic globalization and the creation of the innovative planetary communication infrastructure.

Today, the Internet as an information and communication environment every minute gives the opportunity to generate new ways of communication and knowledge creation, data exchange, transactions between users. In fact, the Internet contributes to the creation of modern social structures and social relations, which are not yet subject to legal regulation in everyday life.

As we know, the Internet consists of millions of interconnected local and global private, public, academic, business and government networks, and is based on the principle of lack of centralized management, rules of use or access. Only the rules for using the Internet Protocol address space and the Domain Name System are centrally defined.

Human identification was initially based on the format of e-mail addresses. However, such a system did not meet the emerging needs of society for reliable user identification, which led to the creation of a variety of systems and types of identifiers, policies and identification schemes. This kaleidoscope of identification technologies and schemes constantly creates legal problems in society related to the legal regulation of identification processes, both at the national and transnational levels.

The general result of these multi-vector decisions is that citizens, organizations, government agencies can not freely and quickly identify their communication partners at the individual level *(Pimenidis, 2014: 2)*.

Due to the lack of a single identification structure, legal entities often have to use a wide range of personal data as identification data *(Cavoukian, 2006: 1)*.

Today, the identification data of the subjects is an important information asset that directly affects public relations in many areas of human life. Also of public importance are the processes of managing the identification data of IoT devices and information technology products with artificial intelligence.

Identification requirements are everywhere and growing rapidly *(Lytvynenko, 2020: 161)*. Users of different systems have various sets of identification data that need to be managed and identified with a specific individual or legal entity. Accumulation of personal and identification data by third parties increases the risks of their illegal use. In fact, identification data has become a strategic resource of any state and requires appropriate physical, technical, legal regulation and protection.

However, the lack of unified technical and legal provisions for the management of identification data hinders the development of the infrastructure of the planetary identity metasystem to replace the existing inefficient set of isolated, incompatible, selective solutions.

It should be noted that the introduction of a single planetary metasystem of a digital identification should not be expected in the near future. This is evidenced by the results of the fourth UNCITRAL working group. Many countries see the creation of an identification metasystem as a repressive measure that could lead to the creation of an authoritarian regime. However, the operation of separate interoperable identification systems is considered more appropriate, which will make the Internet a safer environment and increase its potential to accelerate e-commerce and other digital identity problems.

3. Legal aspects of identification data management

Digital identity management in the electronic world does not have clearly defined legal criteria. At the same time, technological and legal regulation of identification management in a broad sense can be carried out in relation to the specified attributes of identification data of individuals and legal entities, IoT devices and information technology products with artificial intelligence *(Cameron, 2005: 2; Tracy, 2008: 3)*.

However, this can only partially minimize the set of legal issues under the dome of the general problem of identity management. That is, the legal problem of identification data management is the existence of different identification systems and different legal approaches and decisions, both at national and transnational levels.

The development of modern public relations in such areas as e-education, e-commerce, e-medicine, e-banking, etc. is actually constrained by the lack of reliable legal mechanisms for managing identification data that can provide real-time online confirmation of of the subject's compliance with attributes presented, to provide access to information resources.

National information legislation contains more than 4 thousand legal acts that regulate public relations in the information sphere. At the same time, the issues of legal support of public relations based on the use of digital technologies, including the management of identification data, and related to their implementation, are only partially regulated and require further systematic elaboration.

Like most countries in the world, Ukraine needs large-scale reengineering of all electronic resources of the state, modernization of information and communication systems and administrative processes. Ukraine is making some efforts in the direction of technical organization and development of electronic identification processes aimed at purely technical methods of identification. At the same time, the modern national legal framework does not fully reflect the real state of the state's response to social transformation.

A situation has arisen in Ukraine when modern information and communication technologies are rapidly introduced in all spheres of public life in the actual absence of legal institutions for the management of identification and personal data, biometrics *(Bouzefrane, Garri, Thoniel, 2011: 3)*, IoT devices and artificial intelligence.

It is proposed to solve legal problems in the field of identification data management in the following areas.

Develop a unified model of public relations in the field of identity management taking into account the management of identity not only for individuals and legal entities, but also IoT devices and information technology products with artificial intelligence. Lay the foundation for the formation of a legal space of trust – the national domain of trust.

Apply the principle of one of the three main mechanisms of object-oriented programming – encapsulation – in order to develop and create modern legal structures to regulate the field of identity management. That is, to develop modular legal constructions that would have unified legal norms and algorithms for their application in the field of identification data management. Such modular legal constructions are designed to regulate social relations that arise during the application of identification data at different hierarchical levels of legal relations, from conventional to cross-border. The application of such a scheme will allow each organization, government body, state to build a vertically integrated own module, which, regardless of implementation technologies, will ensure the transit of identification data created and legally significant according to national law in a cross-border environment of trust.

It is necessary to formulate the paradigm of identification data management in the context of theoretical and legal principles, namely to present the legal regulation of identification data management processes as self-regulation of complex hierarchical identification systems in conditions of legal uncertainty, with consistent creation and functioning of legal space to a stable stage of development of the sphere of identification data management.

The proposed approaches require large-scale joint work of specialists in the field of information technology, information and other areas of law. In fact, it is necessary to create a new glossary of definitions and norms in the field of identification data management by translating and modernizing technical norms into technical and legal ones. This will provide a logical link between the technical and legal components of the regulatory framework in the field of identity management.

4. Development of a unified classifier of identification data

The first step in this direction will be the development of a unified classifier of identification data. It should be noted that credentials (identification data) are personal data (attributes) of individuals and legal entities that are used for authentication and identification processes in information and communication systems. The class of identification data should also include the attributes of identification of IoT devices and information technology products with artificial intelligence.

Of course, the classification of attributes of identification data should be based on the analysis of methods of identification of subjects and objects, including IoT devices and artificial intelligence, problems and solutions of legal regulation of their application. In our opinion, it is impractical to apply the generally accepted gradations of personal data. Thus, international law recognizes the conditional division of personal data into two groups: data of «general content» and special categories of information, which are defined as «vulnerable» or «sensitive» data *(Romanov, 2010: 42)*.

However, the concept of «sensitive» personal data, which is often used in European Union law and in many decisions of national and international courts (in particular, this term is used in more than ten decisions of the European Court of Human Rights), has not been unambiguously interpreted and doesn't have a comprehensive explanation: why exactly the data of an individual are considered «sensitive». It is extremely rare to ask which categories of data should be classified as «sensitive» and, finally, why they should be given a higher level of protection than other data *(Rizak, 2013: 93)*.

Given the uncertainty with the specific content of «vulnerable», «sensitive» or «hypersensitive» personal data and given that they are used as identification data in information and communication systems, we consider it appropriate to apply their classification on the basis of a colour-coded common hazard classifier.

First, it will allow a clear distinction between data by attribute classes and security levels, as well as levels of threats and consequences in the event of their illegal use.

Secondly, in case of danger a person's imagination intuitively matches certain colors with the level of threat to life – red, orange, yellow, green. Accordingly, it is proposed to divide the attributes of identification data into four groups according to the importance of data for human life, the direction of use and the value of this information resource for the state *(Kostenko, 2021: 22)*.

So the attributes of the identification data of the «red» group, in our opinion, should include the following:

Identification biometric attributes of an individual:

– Static attributes: DNA, skeleton shape, 2D-3D image and facial thermogram, blood type, retina and iris patterns, capillary patterns of palms, fingerprints, ears, characteristics of individual organs, etc.

– Dynamic attributes: voice characteristics, biomechanical characteristics of movements, physiological features of motility, spatial elements (postures, positions, simple joint movements, simultaneous or consecutive movements), information structure of movements (sensory, psychological, reflex, behavioral).

Identification attributes of information technology products with artificial intelligence, cyberphysical systems, ASI class III android robots, super AI: quantum digital signature, control and blocking codes, other identification technologies that will be used to identify AI.

Identification attributes of IoT devices used in neuro / cardio medical devices, military equipment and weapons, in critical infrastructure facilities, the disablement or malfunction of which may pose a critical (fatal) threat to human life and health: IDentifier (OID), Electronic Product Code (EPC), Universally Unique IDentifier (UUID), International Mobile Equipment Identity Identifier (IMEI), ID Key, Qualified Digital Key, Quantum Key.

The attributes of the identification data of an «orange» group should include:

Documentary attributes of a natural person: Name and surname, tax code, passport of a citizen of Ukraine, passport of a citizen of Ukraine for travel abroad, diplomatic passport of Ukraine, service passport of Ukraine, ID-card, seaman's identity card, crew member's identity card, return certificate to Ukraine, temporary identity card of a citizen of Ukraine, driver's license, stateless person's certificate for travel abroad, permanent residence certificate, temporary residence permit, migrant card, refugee certificate, refugee travel document, identity card of an individual in need of additional protection, travel document of a person, which is provided with additional protection.

Identification attributes of a legal entity operating in the field of medicine, defense, state protection and critical infrastructure: name of the legal entity according to the Unified State Register of Enterprises and Organizations of Ukraine, identification code of the legal entity according to the Unified State Register, registration number taxpayer cards or series (if available) and passport number.

Identification attributes of information technology products with artificial intelligence, robots and class AAI, AAII android robots: program codes, external control and blocking codes, other identification technologies.

Identification attributes of IoT devices used in neuro / cardiomedical devices, military equipment and weapons, critical infrastructure facilities, the decommissioning or malfunctioning of which may pose a potential threat to human life and health: Object IDentifier (OID), electronic product code (EPC), universally unique IDentifier (UUID), international mobile equipment identifier (IMEI), ID key, qualified digital key, quantum key.

The following attributes of identification data are proposed to include in the «yellow» and «green» groups: certificates and identification documents issued by non-governmental organizations, any information disseminated by a person of his/her own free will, as well as the legal owner or third party by consent of the above-mentioned carrier of identification attributes, provided that it is informed either by the offer agreement or within the limits of its professional competence (except for the data of the «red» and «orange» sectors).

The list of attributes of the «yellow» and «green» groups may have a fairly large list of identification data used in non-state digital resources.

5. Conclusions

The proposed solutions will contribute to the formation of new social relations and legal rules in the field of identity management and meet the needs of citizens, government and commercial organizations in legal instruments that will ensure the legal significance of transactions using any credentials. This will help increase trust in electronic services, secure identification of entities and objects, and ensure reliable protection of identification and personal data, conditioned upon expedite modernization and alignment of domestic legislation with relevant international standards.

References

Elias Pimenidis. Digital Identity Management 2014 https://www.researchgate.net/publication/259972539.

Cavoukian A. (2006) Laws of identity the case for privacy-embedded laws of identity in the digital age. http://www.ipc.on.ca/images/Resources/up-7laws_whitepaper.pdf.

A. Lytvynenko On the issue of definition and normative content of «sensitive personal data» Scientific Bulletin of Public and Private Law Issue 2,2020 P. 160-172 DOI https://doi.org/10.32844/2618-1258.2020.2.27.

Kim. The Laws of Identity Architect of Identity and Access Microsoft Corporation. http://www.identityblog.com.

Kim Tracy Identity management systems 2008 https://www.researchgate.net/publication/260492739.

6. Marit Hansen. Privacy and identity management. Curity&Privacy. 2008. P. 38-45.

Samia Bouzefrane, Khaled Garri, Pascal Thoniel A user-centric PKI based-protocol to manage FC2 digital identities Le Centre pour la Communication Scientifique Directe 2011 https://hal.archives-ouvertes.fr/hal-00628633

V. Romanov I. Galeuka. On time – biometric identification of a person in Ukraine Worldview № 6, 2010. P. 42-45

M. Rizak. Classification of personal data as a necessary element of the introduction of effective communication in society. Scientific Bulletin of the International Humanities University. Ser. Jurisprudence. 2013. № 6-3. Volume 1. P. 91-95.

O. Kostenko. Identification data: legal mechanisns development of classifiers. Social and Economic Aspects of Education in Modern Society. 2021. P 22.