Tamta Archuadze

DEPERSONALIZATION OF PERSONAL DATA, AS A GUARANTEE FOR THE PROTECTION OF DATA SUBJECT

Tamta Archuadze
Master in Public Law, East European University.

ABSTRACT

In the modern world it is hard to imagine how people could exist without an important personal data protection mechanism – depersonalization – since the life of an individual comprises of such details that, if publicized, would cause immeasurable damage to individual in question and the people around him/her.

This paper looks at how data is defined in a number of diverse categories, discusses the meaning and quality of each category, determines the relevance and importance of legal regulation and examines the practical implementation of depersonalization to fulfill the legislative aim of data subject protection.

In order to study this issue in its entirety, the article reviews the normative base and practice in Georgia as well as the best practices of other countries in creating personal data protection guarantees. This approach makes it possible to analyze the pros and cons of depersonalization as a guarantee for data subject protection.

INTRODUCTION

"Inviolability of personal data is the precondition for the autonomy of an individual, his/her independent development, and the protection of his/her dignity",[1] therefore, it is important to protect the dissemination of any information related to a data subject that may harm him/her in terms of employment, creating a family or even interacting with the outside world.

Depersonalization is an important guarantee for the protection of a data subject. However, its practical implementation is difficult as there is legitimate public interest in informing society about various issues. This means that the data processor must be careful to not spread information that enables the public to identify the data subject.

This article discusses questions of the legal regulation of depersonalization and its practical implementation. In addition, special attention is given to the categories of data that should always be depersonalized should it become necessary to use it in a public form.

The findings in this paper are based on comparative-legal, formal-logical, analytical, historical and sociological research. The comparative-legal research method made it possible to reach a logical and consistent conclusion by comparing and collating positive and negative aspects of laws in several countries. The analytical research method involves problem analysis, which aided my pursuit of consistent and logical arguments and helped me arrive at a rational conclusion. The historical research method helped ascertain the stages of the development of personal data protection legislation. Sociological research was vital due to the fact that personal data is related to society and each individual in society possesses it.

1. THE ESSENCE OF PERSONAL DATA DEPERSONALIZATION AND THE TYPES OF INFORMATION SUBJECTED TO PROTECTION FROM DISSEMINATION

1.1. Definition of personal data depersonalization

The practice of government bodies and various physical entities to collect and process personal information started centuries ago. For instance, even in the Roman Empire, information on tax payers was collected by government representatives and carefully documented on papyrus scrolls. These records provided information taxpayer's occupation, as well as offering insight into real and

1 Decision of the Constitutional Court of Georgia of 10 June 2009 on case N1/2/458, "Citizens of Georgia – Davit Sartania and Aleksandre Macharashvili against Parliament of Georgia and Ministry of Justice of Georgia".

potential enemies of the empire. Taxpayer records have been found for Jesus Nazarene, his apprentices, the leader of slaves – Spartacus – and also about some political and religious activists. In Greek and Egyptian cities, personal data was collected, largely based on information gathered from land registries and the private contracts concluded on the property. This data included information on the racial provenance of citizens in order to differentiate the Jewish, Macedonian, Phrygian, Egyptian and other populations.[2] Experience gained over the course of centuries and the desire to easily identify people led to the introduction of a practice of collecting the most information possible about every living person, which created a threat to the supreme principle of personal privacy.

In 1966 Judge William Douglas stated that people were rapidly approaching an era where there would be no confidentiality; everyone would be subject to surveillance in any time, and nothing would be hidden from the state.[3] In light of the development of technologies, that era will arrive soon.

The increasing tendency in Georgia to collect as much comprehensive information about everyone has resulted in establishing a definition of personal data (which entirely corresponds to the definitions created by developed countries): personal data is information of any kind that serves for the identification of an individual. It may be an identification number, or any type of characteristic – including physical, physiological, psychological, economic, cultural or social features.[4]

Prior to the enactment of Georgian law on "Personal Data Protection", the definition of personal data was included in the "General Administrative Code of Georgia", which considered personal data as the public information needed for the identification of a person,[5] and, in some cases, this was in complete conflict with the necessity of personal data confidentiality.[6]

The Georgian Constitution sets the standard of protecting personal data from disclosure in article 20 paragraph 1 and article 41, without determining its definition. Particularly, article 41 of the Constitution includes a list of the data that is related to the health of a person, his finances or other private issues.[7] Information related to the health of a person is connected to the question of the individual's physical existence; the financial data is connected to his or her life and occupation,[8] and "private issues" is likely linked to the intimate life of a person.[9] According to the interpretation of the Constitutional Court of Georgia, this article of the Constitution "is in connection with the article 20 of the Constitution, by which the inviolability of private life is protected, as it includes such data that is related to the private sphere of a person".[10]

2 Madsen W., Handbook of Personal Data Protection, New York, 1992, 6.

3 Madsen W., Handbook of Personal Data Protection, New York, 1992, 6.

4 Law of Georgia on "Personal Data Protection", article 2, paragraph (a).

5 "General Administrative Code of Georgia", article 27, paragraph (t) (edition of 15.07.1999).

6 "General Administrative Code of Georgia", article 44, paragraph 1 (edition of 15.07.1999).

7 The Constitution of Georgia, article 41 paragraph 2.

8 Decision of the Constitutional Court of Georgia of 30 October 2008 on case N2/3/406,408 "The Public Defender of Georgia and Yong Lawyers' Association of Georgia against Parliament of Georgia".

9 Commentaries to the Constitution of Georgia, Tbilisi, 2013, p. 360.

10 Decision of the Constitutional Court of Georgia of 30 October 2008 on case N2/3/406,408 "The Public Defender of Georgia and Yong Lawyers' Association of Georgia against Parliament of Georgia".

Protection from the disclosure of personal data in cases where public access to certain decisions or collected information is inevitable (for instance: all court decisions are declared publicly;[11] the personal data protection inspector publishes an annual report;[12] the annual report of the public defender is published through the official publishing body of the Parliament of Georgia;[13] information on crimes is spread through mass media etc.), is possible by applying depersonalization or using pseudonyms. Of the two possibilities, the best way to avoid disclosing the identity of the individual in question is depersonalization.

Generally, it is important that depersonalization is applied in cases when the information related to a fact, event, person and others will be accessible to public. If the possibility of disclosure was not an issue, depersonalization would not have become necessary, since the information in question would not have left the domain of the data processor.

Complete depersonalization, which implies a data anonymity mechanism that makes it impossible to identify the subject, is practically unattainable,[14] therefore the legislation considers depersonalization as the modification of information to the degree that would make it impossible to link it to the data subject, but at the same time seeks to address the circumstances, when anonymity may not be secured entirely. In such a case, exposing the link between the data and person must require a disproportional amount of effort, expense and time.[15] The Federal Data Protection Act of Germany includes a nearly identical definition of depersonalization.[16] This is known as practical depersonalization ("faktische Anonymisierung"),[17] as total depersonalization depends on the actual implementation of the act; legislation is just the legal framework that defines the means of data modification to hide the subject's identity.

The legal definition of depersonalization is not included in the acts on personal data protection in most countries; the best definition can be found in Germany and Georgian legislation on personal data protection. In Ukraine, the act on personal data protection also defines depersonalization, but very briefly: depersonalization means eliminating information that directly or indirectly identifies a person.[18]

Some countries, however, opt not to define depersonalization if the government agency that processes or maintains data on the state's citizens modifies that information to the extent that the data subject is protected from exposure.

11 Criminal Procedure Code of Georgia, article 10, paragraph 2.

12 Law of Georgia on "Personal Data Protection", article 38, paragraph 1.

13 Organic Law of Georgia on "Public Defender", article 22, paragraph 2.

14 Fischer-Hübner S., IT-Security and Privacy: Design and Use of Privacy-Enhancing Security Mechanisms, Berlin, Heidelberg, New York, Barcelona, Hong Kong, London, Milan, Paris, Singapore, Tokyo, 2001, 112.

15 Law of Georgia on "Personal Data Protection", article 2, paragraph (r).

16 See. Federal Data Protection Act in Germany, section 3, paragraph 7.

17 Fischer-Hübner S., IT-Security and Privacy: Design and Use of Privacy-Enhancing Security Mechanisms, Berlin, Heidelberg, New York, Barcelona, Hong Kong, London, Milan, Paris, Singapore, Tokyo, 2001, 112.

18 Law of Ukraine on Protection of Personal Data, article 2, sentence 6.

1.2. Categories of data subjected to depersonalization and legal standards of confidentiality

1.2.1. Information relating to the special category and means of protection from disclosure

Prior to the adoption of the Georgian law on "Personal Data Protection", the legislation did not contain a special status for any type of personal data or stricter regulation for its protection. However, under the influence of developed countries, in 2010 the Supreme Court of Georgia ruled to define personal data according to two categories – sensitive and ordinary data – and underscored that "personal data in the sensitive category differs from ordinary personal data under a special legislative regime. The processing-distribution of such personal data requires consent from the relevant person".[19] This definition was exceptionally progressive, considering the limited regulations regarding personal data protection that existed at that time.

Nowadays the existence of personal data protection legislation that does not protect information deemed to be "sensitive, and of special category"[20] – related to a person's racial or ethnic identity, political views, religious or philosophic beliefs, enrolment in professional union, health condition, sex life[21] – is inconceivable. According the directive of European Parliament and Council, this short list is the minimum that must be included in the personal data protection legislation of every country; therefore there is an expectation that member states of European Union will expand the list of special category information and will strengthen the regulations, as they are free to implement stricter rules.[22]

Considering Georgia's aspiration to become a member of the EU and comply with European standards, the Georgian law on "Personal Data Protection" is very comprehensive. It not only protects the minimum of special category information, but also includes additional information concerning any convictions, administrative custody or imprisonment as well as any plea bargaining, probation, recognition as a victim or damaged from crime that a person may have experienced in his or her lifetime. Information related to biometric and genetic data is also covered.[23]

As a rule, laws related to personal data protection in most countries define the special meaning of information connected to criminal law processes.[24] The most comprehensive is Estonia's "Personal Data Protection Act", which includes information obtained during criminal law case proceedings

19 Decision rendered by the Chamber of Administrative Cases of the Supreme Court of Georgia, dated of 5 July 2010, Nbs-1278-1240 (k-08).

20 Brouwer E., Digital Borders and Real Rights: Effective Remedies for Third-Country Nationals in the Schengen Information System, Leiden, Boston, 2008, 2012.

21 Directive 95/46/EC (Grand Duchy of Luxembourg, Luxembourg) (in force from 13.12.1995), Article 8.

22 Klosek J., Data Privacy in the Information Age, Westport, Connecticut, London, 2000, 31.

23 Law of Georgia on "Personal Data Protection", article 2, paragraph (b).

24 E.g. see ,,Data Protection Act 1998" of UK part I, paragraph 2, part h), ,,Law On Legal Protection Of Personal Data" of Republic of Lithuania, article 2, paragraph 9, ,, Personal Data Act (523/1999)" of Finland Chapter 3, Section 11, part 6), ,,The Greek Data Protection Law of 1997 (Law 2472/1997)" Article 2, paragraph b) etc.

or during other proceedings related to crime in the category of sensitive information, protecting it from disclosure until a public court hearing takes place or a decision is made. Information that includes social morality, private or family life; less important issues; the identity of a victim and damages inflected upon them; and any other data that is protected from disclosure according to the law, are also considered sensitive.[25] Unlike the Estonian "Personal Data Protection Act", the Georgian law on "Personal Data Protection" names the data related to a criminal law procedure as part of the sensitive category, due to the fact that this information is not included in the criminal code. The data listed includes personal data of special category, specifically information connected to previous convictions, administrative imprisonment, detention, plea bargaining, probation, recognition as a victim or injuries as the result of a crime.

Data that falls within the special category is given the highest standard of protection and cannot be processed[26] without the written consent of the data subject except in certain circumstances, including: employment issues; protecting the interests of a third person; health care; and court cases.[27] Considering that special category data is highly sensitive and is classified as confidential information,[28] despite the lawful access of the data processor, it is prohibited to publish or disclose to any third person the information collected without consent of data subject – with the exception of the circumstances listed above.[29] Therefore, data processor shall be empowered by law or an agreement with the data subject to allow it to process data that has been defined as part of the special category.[30]

1.2.2. Biometric data and standards to restrict its disclosure

The question whether biometric data is personal information has long been the subject of discussion. The dispute is based on two issues: first, biometric samples are mostly medical information and represent a key to access personal information and, second, biometric data is produced by a person's behavioral and psychological characteristics, which links the data to a particular individual and turns it into personal data.[31] Regardless of whether biometric data is considered to be personal data or not, the main purpose of the processors of such data is to have access to the personal information existing about a data subject. Therefore, the protection of biometric data and, in some cases, the decision to define it to the special category,[32] is motivated by the scale of the information collected and the particularities of the interest in it.

25 Estonia: Personal Data Protection Act, article 4, paragraph 7.

26 Law of Georgia on "Personal Data Protection", article 6, paragraph 1.

27 Law of Georgia on "Personal Data Protection", article 6, paragraph 2.

28 "Who Owns Our Genes?": Proceedings of an international conference, Tallinn, 1999, 78.

29 Law of Georgia on "Personal Data Protection", article 6, paragraph 3.

30 Law of Georgia on "Personal Data Protection", article 16.

31 Nanavati S., Thieme M., Nanavati R., Biometrics: Identity Verification in a Networked World, New York, Chichester, Weinheim, Brisbane, Singapore, Toronto, 2002, 243.

32 Law of Georgia on "Personal Data Protection", article 2, paragraph (b).

The grounds for serious biometric studies were laid in the 1960s, while the technology developed and improved in the 1970s to 1980s. Significant development started in the mid-1990s.[33]

The Georgian law on "Personal Data Protection" considers biometric data to be personal data and defines it as a physical, psychical and behavioral feature of a person that is unique and permanent for each individual and can be used to identify him/her (fingerprint, footprint, color of the eye, membrane of eyeball – an image of the eyeball, characteristics of the face).[34]

Generally, the list of physical biometric data is much longer and has been used for many years. As early as 1960, data from an individual's hand was used as a mean of identification. Athletes identified themselves using a hand scan at the 1996 Atlanta Olympic Games. Today, however, hand scans are rarely used.[35]

The most actively used type of physical biometric data is the fingerprint, which is unique to every person and permanent. It was first used in the criminal law system, where initially fingerprints were studied and classified manually. By the 1960s, however, after the invention of computers, experiments using biometric fingerprints began at the US National Standardization Bureau. In 1979 the US Federal Bureau of Investigation examined the first test sample of the fingerprint searching system. By 1983, the Automatic Fingerprint Identification System (AFIS) was regularly used.[36]

The possibility of identifying a person by his or her voice was first raised in 1963, however it wasn't until 1974 that the technology was tested by US telephone and telegraph company in its research laboratories.[37]

People frequently use facial appearance for confirmation of their physical identity (e.g. identification card and driving license, passport and other identification documents usually include the individual's photograph), and the idea of using the face as biometric data was actively discussed after Helen Chan and Charles Bisson published their first studies on the issue in 1965. Research into an automatic face recognizing system started in Canada in 1977, but there were no significant breakthroughs until the 1990s, when companies like Cognitec, ZN, Viisage Technology and Visionics Corporation started producing commercial systems of face recognition. By 2004, the technology needed to study the "texture of the face" had already been developed.[38]

The development of technology to identify a person using the membrane of the eyeball started in the mid 1970s. Two ophthalmologists, Leonard Flom and Allen Safir,[39] developed – and later pat-

33 Dunstone T., Yager N., Biometric System and Data Analysis Design, Evaluation, and Data Mining, Eveleigh, NSW, Australia, 2009, 5.
34 Law of Georgia on "Personal Data Protection", article 2, paragraph (c).
35 Dunstone T., Yager N., Biometric System and Data Analysis Design, Evaluation, and Data Mining, Eveleigh, NSW, Australia, 2009, 6.
36 Dunstone T., Yager N., Biometric System and Data Analysis Design, Evaluation, and Data Mining, Eveleigh, NSW, Australia, 2009, 5.
37 Dunstone T., Yager N., Biometric System and Data Analysis Design, Evaluation, and Data Mining, Eveleigh, NSW, Australia, 2009, 8.
38 Dunstone T., Yager N., Biometric System and Data Analysis Design, Evaluation, and Data Mining, Eveleigh, NSW, Australia, 2009, 7.
39 Dunstone T., Yager N., Biometric System and Data Analysis Design, Evaluation, and Data Mining, Eveleigh, NSW, Australia, 2009, 8.

ented – the technology to identify an individual by scanning the iris of his or her eye. This method has its challenges, particularly when the subject is a child or someone who is ill.[40]

Other types of biometric data also exist, including: the so called keyboard dynamics, which allow a person to be identified based on the rhythm of how he or she types on a keyboard;[41] the 3D face image was first used as a biometric sample in 1992 and involves using cameras to study a person's face down to the tiniest detail;[42] and the hand palm print, first used in Hungary in 1994 and now done by AFIS.[43]

Studies related to the identification of a person and the gradual increase of the information linked to the biometric data proved that an individual's unique features are limitless and technology alone determines when and how they will be used for research. Eventually it will be possible to identify an individual using even more types of biometric technologies, such as scanning blood vessels; face thermography; setting compliance of DNA; and determining body odor, blood pressure, walking manner and the form of a person's ear.[44] It is widely expected that, as technology advances, new types of biometric data will also be developed. Therefore, most countries do not list the types of biometric data that will require special protection in data protection laws; rather they define generally unique and permanently existing physical, mental and behavioral features as biometric.

Based on the informative nature of biometric data, the Georgian law on "Personal Data Protection" defines different regulations for the processing of biometric data by public and private institutions and stipulates that the processing of such data is only possible for purposes involving the security of an individual, the protection of property and should not be accessible in any other circumstances. The legislator has unlimited rights to process biometric information in accordance with the law on the issuing of an identification document or the identification of person crossing border as well as other circumstances directly prescribed under Georgian legislation. The law requires that private institutions provide information to the personal data protection inspector and the data subject before using biometric data.[45]

The Georgian legislator stipulates special regulations for processing biometric data, since it is important that the information remains confidential and is not released to the general public. The identity of the data processor and the framework for processing biometric data are both strictly defined. It is also noteworthy that the law includes additional obligations for private institutions that process biometric data, specifically the responsibility to inform the personal data protection inspector before using the processed data, while public institutions are not obligated to do so. An important distinction is when the information is necessary as part of a covert police operation. In

40 Newman R., Security and Access Control Using Biometric Technologies, Boston, 2009, 42.

41 Newman R., Security and Access Control Using Biometric Technologies, Boston, 2009, 53.

42 Dunstone T., Yager N., Biometric System and Data Analysis Design, Evaluation, and Data Mining, Eveleigh, NSW, Australia, 2009, 6 and 64.

43 Dunstone T., Yager N., Biometric System and Data Analysis Design, Evaluation, and Data Mining, Eveleigh, NSW, Australia, 2009, 5.

44 Newman R., Security and Access Control Using Biometric Technologies, Boston, 2009, 53.

45 Law of Georgia on "Personal Data Protection", articles 9 and 10.

that case, the prosecutor involved in the investigation must notify the personal data protection inspector about the activities already implemented or to be executed[46] that concern processing personal data. In fact, even the Georgian National Communications Commission is legally obliged to register any instances that the data is discussed through telecommunication networks to the state institutions and to pass the necessary information to the personal data protection inspector.[47] In all other cases, i.e. any other public service that requires the use of personal data, the law requires that the data processor takes the necessary steps to ensure the information is not disseminated to the wider public.

1.2.3. Genetic data and confidentiality standards

Genetics is the study of heredity and the variation of inherited characteristics.[48] The field started in 1860 thanks to the work of Gregor Mendel, who first proposed the existence of genes.[49] A gene is the double twisted molecular thread, known as deoxyribonucleic acid or DNA.[50] In 1953, after Watson and Crick discovered the structure of DNA, molecular genetics were used to explain the flow of vital processes.[51] The discovery of genes, their molecular structure and functions has allowed us to comprehend the two biggest secrets of biology: 1. What makes a species appear as they appear to us? (It has been shown that genetic inheritance is decisive, for instance cats always give birth to cats, etc) and 2. What causes the differences within a species? (For instance animals with unique coloring frequently have descendants of the same color, with the same characteristics, which means that they are particularly "produced only from this family").[52] Therefore, genetics is the means for "surveying" an organism.[53] Through genetics it is possible to find unique and permanent information which is particular to an individual subject and his/her blood relations.[54] Knowledge about one's genetic data may help an individual avoid or significantly minimize hereditable diseases;[55] however the public disclosure of this information may lead to a particular individual being excluded from society.

The Georgian law on "Personal Data Protection" defines genetic data as the "unique and permanent data of a data subject on genetic heredity and/or DNA code, by which the identification of a person is possible".[56] This means genetic data is part of the special category.

46 See Criminal Code of Georgia article 143^3 paragraphs $5,6^1$, 7 and article 143^8 paragraph 3.

47 Decree N2 of the Georgian National Communications Commission "On approval of the Statute of Georgian National Communications Commission", article 7, paragraph 3, subparagraph (l).

48 https://en.oxforddictionaries.com/definition/genetics

49 Griffiths A., Miller J., Suzuki D., Lewontin R., Gelbart W., An Introduction to Genetic Analysis, New York, 2000, 23.

50 Ibid. 3

51 Human Genetic Information: Science, Law and Ethics, UK, 1990, 6.

52 Griffiths A., Miller J., Suzuki D., Lewontin R., Gelbart W., An Introduction to Genetic Analysis, New York, 2000, 3.

53 Human Genetic Information: Science, Law and Ethics, UK, 1990, 7.

54 Ibid. 6

55 Ibid. 96

56 Law of Georgia on "Personal Data Protection", articles 2, paragraph (c^1).

Some genetic data, such as genetic inconsistency and inclination to serious diseases, is particularly sensitive, compared to other types of genetic information, such as sex, color of hair and eye, which is less sensitive. However, it is possible that attitudes towards this information will change. For instance, some parents are not provided with information on the sex of the embryo,[57] if the concern exists that the family could decide to abort the pregnancy based on the sex of the fetus.

DNA samples of a human's cellular tissue, as a determinant of person's individuality, will be always considered confidential, as far as its disclosure could result in revealing exceptionally sensitive information,[58] or "family secrets" such as parentage and adoption.[59]

The Georgian law on "Personal Data Protection" does not provide any special regulations with regard to the processing of genetic data; however the regulation of processing special category data applies to genetic data as well, as the definition of the abovementioned includes genetic data. Consequently, the protection of genetic data is as strict as any other data of special category.

2. PROBLEMS IN THE PRACTICAL IMPLEMENTATION OF DEPERSONALIZATION

As the legislative definition of depersonalization must include the possibility of practical implementation, it is necessary that several legal preconditions exist to ensure implementation. For instance, in the decision on the census of the population, Constitutional Court of Germany requested early practical depersonalization of the census data to exclude the possibility that a data subject could be identified: According to section 40, paragraph 3 of the Germany Federal Data Protection Act, personal data in the possession of research institutes "shall be depersonalized immediately whenever the research purposes make it admissible". Up until that point, the information identifying data subjects must be stored separately. If the separation is not performed, at least it must be substituted by pseudonyms directly (or if possible indirectly).[60] Without the implementation of preventive protection measures, identity thieves who possess additional data on a person's identity (name, surname, address, personal number), demographic features (sex, nationality, education, religion, family status), medical data (diseases, habits), etc, could identify data subject and disclose his/her sensitive personal data.[61]

57 "Who Owns Our Genes?": Proceedings of an international conference, by Nordic Committee on Bioethics, Tallin, 1999, 78.

58 Ibid. 78

59 Stefanick L., Controlling knowledge: Freedom of Information and Privacy Protection in a Networked World, Canada, 2011. 101.

60 Fischer-Hübner S., IT-Security and Privacy: Design and Use of Privacy-Enhancing Security Mechanisms, Berlin, Heidelberg, New York, Barcelona, Hong Kong, London, Milan, Paris, Singapore, Tokyo, 2001, 112.

61 Fischer-Hübner S., IT-Security and Privacy: Design and Use of Privacy-Enhancing Security Mechanisms, Berlin, Heidelberg, New York, Barcelona, Hong Kong, London, Milan, Paris, Singapore, Tokyo, 2001, 113.

For statistical, scientific and historic purposes, the obligation of protecting the interests of a data subject during data collection is stipulated by the Georgian law on "Personal Data Protection",[62] however it does not oblige the person processing the data to depersonalize the collected information, which is a shortcoming that should be corrected. As it stands, the practical mechanism to protect information from disclosure is limited to the requirement that a personal data protection inspector carry out the depersonalization of data, "if he/she considers that processing of data is not performed in conformity with legislation".[63] The problem arises when personal data becomes available to outsiders before it has been depersonalized and before an inspector is informed about the breach. The Georgian law on "Personal Data Protection" does not include uniform regulation dictating how to protect a data subject's identity from disclosure; in practice, this is possible through encryption, withholding or concealing information or assigning pseudonyms, as well as other methods. Assigning an individual a pseudonym is mostly done in criminal law procedure with the purpose to protect the individual involved, particularly, if the person is under special protection measure. This includes individuals who witnessed a crime and are in protective custody. Steps can be taken to conceal his or her identity, such as referring to the individual by a pseudonym; changing his or appearance; and classifying procedural documents including those that make it possible to identify or recognize the person.[64] As it is prohibited to disclose and publish the personal data of juvenile, except in cases prescribed by the law on "Personal Data Protection",[65] people processing data are obliged to assign a pseudonym, use the juvenile's initials, encode the information or use other method to ensure the individual's identity remains protected

3. MECHANISMS OF RESPONSIBILITY FOR NOT PERFORMING DEPERSONALIZATION

The right of a data subject to depersonalize his/her personal data in cases defined by Georgian law must be protected and guaranteed; the personal data protection inspector is obligated to, upon receipt of the relevant request, follow the depersonalization measures as prescribed by law.[66] An inspector, even without notification from a data subject, also has the right to require depersonalization under his/her initiative if he/she has reason to believe that the data processing is being done illegally.[67]

62 See Law of Georgia on "Personal Data Protection", article 7, paragraph 5 and article 15, paragraph 4.

63 See Law of Georgia on "Personal Data Protection", article 39, paragraph 1, subparagraph (c).

64 Criminal Procedure Code of Georgia, article 68, paragraph 3, subparagraph (b).

65 Law of Georgia on "Juvenile Justice Code", article 13, paragraph 2, sentence 2.

66 Law of Georgia on "Personal Data Protection", article 34, paragraph 1.

67 Law of Georgia on "Personal Data Protection", article 39, paragraph 1, subparagraph (c).

: It is worth noting that the personal data protection inspector does not have to justify his/her decision to depersonalize data. In fact, the data processor has the right to depersonalize data even when there is a legitimate public interest in this information. For instance, decisions by common courts are usually published using the initials of the parties involved – even though court hearings are public and anyone could attend and learn their identities.

There were only two situations when a personal data protection inspector has required depersonalization of the data: in order to ensure compliance with international election standards and in order to create an accessible environment for persons with disabilities to vote.[68]

In 2015 report by the personal data protection inspector describes two occasions, when the court issued copies of a judgment as public information using only the initials of the parties involved, without personal data, however, due to the nature of the judgment, it was possible to identify the citizens involved and reveal information that belonged in the special category.[69] This experience illustrates that depersonalization is not just a matter of concealing data such as someone's name or personal identification number; true depersonalization is making the data anonymous.

A personal data protection inspector has two instruments to reinforce the law: warnings and fines. The amount of the fine depends on what kind of personal data was processed illegally and whether a second instance of illegally personal data processing has taken place following the initial warning or fine.[70] The law does not consider the volume of amount of data that was illegally revealed. The amount of the fine is fixed regardless of the scale of the damage. However, it is important to take into consideration that the illegally disseminated data may be worth more than the fine imposed. The best regulation would be if a personal data inspector had the right to study each case individually and determine the amount of the fine based on the scale of the violation.

If a person's right to depersonalization has been violated, the individual in question is allowed to seek justice through the proper authorities, including through the court system.[71]

Out of the cases involving personal data protection that have been heard in Georgian courts, one particular case, involving the Rustavi city assembly, stands out. The judge hearing the case refused to allow the publication of the data in question. In this decision, the court discussed certain articles of the Constitution while talking about disclosing data of a distinct category, notwithstanding the fact that by that time the special law was enacted, however it uses law on "personal data protection" as well. This decision is important as it defines a legal precedent for issuing personal data about individuals determined under article 2 of the Georgian law on "Conflict of Interest and Corruption in public service" and determines that publishing information related to public officials (as well as their family members), including confidential information, serves a legitimate purpose

68 Report of the Personal Data Protection Inspector "Condition of Personal Data Protection in Georgia", Tbilisi, 2014, 15.

69 Report of the Personal Data Protection Inspector "Condition of Personal Data Protection in Georgia", Tbilisi, 2015, 26-27.

70 See Law of Georgia on "Personal Data Protection", chapter VII.

71 Law of Georgia on "Personal Data Protection", article 26, paragraph 1.

– provide transparency of information on public officials.[72] Based on this definition, the court considers that disclosing any kind of information on public official is justified; however regardless of the individual's status and the increased public interest, it is necessary to ensure that some of the information that is available has been depersonalized and can only be publicized if the data subject has given consent.

It shall be noted that the courts have largely weighed in on issues of data protection when it related to issuing information as well as refusing to provide and process data. The issue of the requirements for depersonalization and its legality has not been discussed in court yet.

CONCLUSION

Georgia is just beginning to create personal data legislation and it is to its credit that the country is following the standards that have been set by other countries and international organizations. In some areas, like the definition of depersonalization, Georgia is at the forefront.

This article sought to demonstrate that depersonalization is the best way to protect a data subject from exposure. That means it is necessary for Georgia to continue to improve how depersonalization is implemented, so that the practice becomes consistent with the legal definition.

The examples used in this paper illustrate the need to resolve the problem of disclosing data that should be depersonalized. This problem continues to exist due to problems in the systems like the courts, and the poor example they set undermines efforts to ensure that other public and private organizations follow the law on depersonalization.

There is ample evidence that the personal data protection inspector is working well; the agency immediately and correctly reacts to violations of the law on the personal data protection inspector. It would be better, however, if depersonalization cases were thoroughly studied by the personal data protection inspector because incorrect depersonalization harms public interests. For example, there is information which the public has the right to know but it has been depersonalized due to incorrect decisions.

In addition, the issue of imposing fines when there are violations should be reviewed. Namely, the inspector should have the right to determine the amount of the fine considering the damage that was caused by the infringement and the benefit received by the data processor. This will lead to a detailed study of every case and the implementation of fair punitive measures.

72 Decision made by the Administrative Chamber of the Supreme Court of Georgia, Nbs-527-518 (k-12) from 30 May 2013.