The Human Rights: The Legal Protection of Personal Data

PhD. Ervin Karamuço

Albanian University, Department of Law and Political Science, Tirana, Albania
Email:ekaramuco@yahoo.com

Doi:10.5901/ajis.2015.v4n2s2p224

Abstract

This paper handles a fundamental human right, with a development dynamic that made it increasingly important in the life of every individual in a society. Considering all the issues in the implementation of personal data protection standards in our country, it is aimed to analyze one of the broadest sectors in the collection and processing of personal data, and the problems that arise during the exercise of public administration institutions' activities. The reasons that led us to such a research are also related to the collusion of the right to privacy and the right to collect and process personal data by public institutions (during their activities and for the fulfillment of rights of citizens themselves), analyzing the legal requirements to guarantee this right and the control for its full implementation by the subjects of the data themselves. In the conclusions part, it is aimed at providing answers to the above issues, as well as producing recommendations based on the analysis of the material conditions in the formal guaranteeing of this right or on the problems encountered in practice.

Keywords: *Personal data, human rights, public authority, information, data security*

1. Introduction

Bearing in mind the category of persons that might have the status of the controller of personal data (this can be any individual, legal entity, public authority, agency or other body that, jointly or individually determines the objectives and manners of personal data protection in compliance with the laws and secondary legislation of this area and is responsible for implementing the obligations defined by law), the administered data can be classified as per the sector their controllers operate in, by dividing them in private sector controllers and public sector controllers. One of the main controllers is precisely the public administration. The later, composes the organizational and professional apparatus, excluding institutions falling out of the scope of the law on the organization and functioning of the state administration (Law no. 90/2012), that serves the public interest, impartially, implementing the legislation in power through performing public services, and drafting and implementing the general state policies. The public institutions represent the system of bodies and mechanisms that mediate and manage the lively activities of any individual in the society, which collect and process personal data at central or local level as a need related to complying with public interests or exercising the powers of such bodies. Thus, the public administration bodies keep different records which, partially or fully, have to do with citizens' personal data (e.g. data on persons born, married, dead, records on tax obligations etc.). Considering this expansion, the protection of citizens' personal data as a guaranteed constitutional right, constitutes an important issue in the framework of the daily activity of a vast number of public sector bodies.

In handling the relationship created between any data controller, specifically the public one, and the subject of data, it is inevitable to determine criteria which are primarily related to the quantitative criteria and the material power to process data. Thus, personal information corresponding to any individual's expectations is guaranteed, and the authority and public image of state institutions as guardians of lawfulness in terms of private life and civil rights protection is created. Our country applies rules that are formalized in important domestic and international acts and documents building on the experiences of the developed countries of Europe. The administration of personal information by public bodies is any action or group of actions made on personal data, through automatic means or otherwise, starting from the gathering of personal data and continuing with all legal forms provided for their processing registering, organization, maintenance, adaption or change, return, consulting, use, transmission, distribution or availability, extension or combination, photographing, mirroring, entry, completion, selection, blocking, annihilation or destruction. These data are collected mainly from the data subject in the form of the obligations set forth by the administration to fulfill the responsibilities of these bodies as well as a prerequisite for obtaining the services desired by citizens. Given the sensitivity of this activity for every individual, in every country rules are set to define the extent of the obligations of the

individual and the conditions in which they are collected to be processed, for certain duration and with previously defined goals. For this reason, this process is guided by the principles that establish the framework of lawfulness of the activity of the public administration in the event of processing personal data to implement the legislation in this area. Also, as noted in their systematic interpretation, it is understandable that these general rules affect the most sensitive aspects of the legal nature itself of these relationships.

The due process of personal data processing for each individual is based on the legality of the purpose of processing; in the collection for specific, clearly defined, and legitimate purposes, and in the processing in accordance with these purposes; in the adequacy of the data, which should be within the scope of the processing and do not beyond that purpose; the accuracy of the data, and when necessary their update; undertaking reasonable actions to delete or correct inaccurate or incomplete data, related to the purpose for which they were collected or are further processed; in maintaining them in such a form that allows the identification of data subjects for specific period of time, but no more than what is necessary for the purpose for which they were collected or further processed. And to conclude with the importance of these principles, the Law no. 9887, dated 10.03.2008, as amended by Law no. 48/2012 "On the protection of personal data" sets through binding provisions that the controller is responsible for the implementation of these requirements in all data processing, be it automatically or by other means.

In any event, the analysis of the relationship that exists between any subject whose data are processed by each public institution for various reasons and interests remain in the focus of the treatment of two important aspects.

Firstly,this relates to the nature of the personal data itself and of the information obtained from them, which constitutes one of the dimensions of the life of every individual (Bennett, C.J. Raab, C.D, 2003). Hence, these data and the rights related to them constitute one of the fundamental human rights, such as privacy. In anyone's objective to have their personal space intact, naturally arises the claim to consider the information about the private life of the man as intact or inaccessible especially by public entities (Halpern, S. W, 1988). Based on definitions of the European Court of Justice (Leander v. Swede, 1987, Kopp v. Switzerland,1998; Amann v. Switzerland, 2000) the processing of personal data from certain categories of controllers who follow and implement public interest, guaranteeing the rights of individuals is protected by proportional balancing of the interests of the different entities involved.This balance principally relies on the principle of complete protection of personal data even if the purpose of processing personal data by public controllers is related to a legitimate interest. What constitutes a key element in such a collision of rights, is the requirement for the individual's personal interest not to prevail (Henkin, L, 1974). As noted, it requires a careful evaluation of hypotheses, which relates not only with the prevailing of the public interest, but also with the level of violating the privacy of the individual through data processing. In this regard we find room to bring to attention a special category of subjects in society, such as children, whose data processing for the sake of their legal positions in certain ages is not specifically addressed by the Albanian legislation. However data processing for children with the consent of their legal representatives requires a more specific protection.

The second aspect relates to the legitimate interest of any institution to process personal data and requirements that must exist to prevent or stop the violation of personal data. In this regard, in the following part of the paper we intend to analyze what the obligations of public institutions are in any case of data processing and the rights of subjects on their data. Undoubtedly, through these mechanisms it is aimed at attention and double protection of data, but as will be seen from the analysis, there are social,political and legal factors that influence in the form of essential gaps and/or abuses in this regard.

2. Research Methodology

This is a theoretical research, based on data achieved by studying legal provision and international court decisions. In order give a full picture of legal data protection many laws, books and scientific articles were studied, concerning to the issue.

3. Official access to personal data

The legal bond arising between the authorities of the state administration on the one hand and on the other hand citizens, with the scope of processing personal data reflects all the characteristics of the relationships with a public character, in all hypotheses of their existence. In these relationships, public institutions operate as vested with rights and duties, which certainly put them in an unequal position compared to data subjects (Hixson, R. F, 1987). From the content of these relations, namely through the organization and functioning of state bodies we benefit the realization of different interests

of society. As a result, they mediate and manage the social activity of each individual making necessary accessing personal data for the purpose of exercising the powers defined by law. In this regard personal information becomes a prerequisite for the fulfillment of their specific obligations in all aspects of public governance.

Such are the services received from the activity of public administration bodies at the request of citizens or organizations to give reports, issuing certificates, sketches, drawings or other documents or conducting relevant activities for the recognition, exercise or performance of certain rights and obligations. Given the correlation that exists between personal data and information received from them, we can say that information is the subject of any administrative service. The rights and obligations of public institutions on personal information collected constitute an objective factor in the realization of the rights or obligations of the private entities, data subjects. A special place in these processes is dedicated to the mechanisms provided for the protection of personal data by public controllers and reserved rights to data subjects to ensure their double protection.

Based on the law no. 9887, dated 10.03.2008, as amended by Law no. 48/2012 "On the protection of personal data" and the secondary legislation adopted by the Commissioner for Personal Data Protection, which is an independent authority in this area, it is provided for the principles of data protection in public administration and issues that should be considered before collecting and processing data. In view of data protection, the controller - the public authority - must apply the principles to be applied in each case of data processing provided for in Article 5 of the law concerning the legitimacy of special processing processes, data proportionality between data gathering and processing and the final goal, the principle of good will. All the aforementioned principles emphasize the establishment of requirements which minimally relate to defining the processing purpose and the content of data files to be administered by them. In this way the development of administrative processes in conformity with modern trends is enabled.

The right of public authorities to operate over personal data is regulated in such a way that boundaries or definitions of the conduct of these authorities towards accessible information and results of their activity are set. In substance, their activity concerning data processing intends to comply with certain obligations which influence the establishment of an area of action, security, or lawfulness, in favor of economic and social progress, effectiveness of the public administration and guaranteeing citizens' personal freedoms in society.

As a logical continuation of the above, it is worth emphasizing the importance to be given to the appropriate level of personal data for their processing and consequently to the performance of duties that state institutions perform in the public interest or for their functioning. Any processing of personal data is a violation to privacy and therefore this violation should be carefully limited as much as possible. For this reason, the controller has no right to process data except for the data that is definitely necessary to be processed for the performance of his duties. Given the somewhat subjective dimension related to the extent of the need to process data, the legislator's intentions regarding the content of the principle of proportionality or adequacy must be clarified. Based on the analysis made, the bylaws of the Commissioner for Personal Data Protection (Instruction no. 37, 2013) reflect a generalist definition of such requirement or lack of doctrinal treatments to refer to. In the literal interpretation of the legal provision on the adequacy of the data and on avoiding exceeding the scope of processing, we note the existence of a direct connection of two criteria: the purpose of processing and the amount of data needed to fulfill this purpose. Overall, the implementation of this principle is exhausted in an insufficient level of security. Based on the European Convention no. 108, dated January 28, 1981 "On the protection of individuals with regard to automatic processing of personal data", in chapter II, the principle of adequacy is ranked among the fundamental principles of the protection of personal data. According to Article 5, letter "c" of the Convention 108, the object of the automatic processing should be adequate, relevant and not excessive in relation to the purpose for which personal data was stored.

Also, based on the spirit of Directive 95/46/EC of the European Parliament and Council of 24 October 1995 on the protection of individuals from the automatic processing of personal data and on the cross-border movement of this data provides for the obligation of Member States to ensure that data should be adequate, relevant, and not excessive in relation to the purposes for which they were stored.

So, the principle of adequacy is closely linked to the principle of specification of the purpose (the principle of limited scope). It should be underlined that the definition of the scope and assessing the adequacy of personal data should be made no later than the moment of collection of such data. The controller is responsible for all automatic or by other means processing of data, which become the subject of administrative proceedings only if and as far as the purposes set by the public institution cannot be achieved without processing information including personal data. The principle of adequacy guarantees the data subject that the controller saves the data file, using only the minimum necessary data (only the data necessary to achieve the purpose intended). In such cases, the level of interference in personal life is minimal. On the other hand the definition of the purposes of data collection should be adequate, relevant and specifically

limited.

On the other hand the existence of a legitimate public interest in the right of public institutions to access data associated with a natural person who is identified or can be identified, directly or indirectly, by an identification number of one or more specific signs, should ensure effective governance, national security, public order, fighting crime or preventing abuse of power by individuals vested with public power etc. According to the sector model of personal data processing (Daniel J, Chris, J. H , 2006), the specific legislation determines the obligation of individuals to provide personal data and the right of public authorities to enter into those data justifying access especially given the interest in the proper performance of the administration's duties, thus contributing to satisfy personal interests of individuals in the areas of education, health, social policy, security etc. Any public controller is obliged to protect the information collected in the performance of his duties, and inform the fulfillment of the requirements laid before him. In this respect not only the data collected and processed, but also the facts and circumstances arising from the process of their mental processing, again represents personal information, subject to the right to privacy.

4. Data security

Security is not just about physical measures, but also has to do with the organization of work in such a way as to minimize risk and personal details are kept safe and not misused or corrupted in any way. Based on Decision No. 6, dated 08.05.2013 "On establishing detailed rules for the provision of personal data", binding rules are set for implementation by public and private controllers. According to this Decision, the controller is obliged to define the categories of personal and sensitive data being processed, to determine levels of access to data in accordance with the job profile, in view of the data processing and protection, implement policies regarding privacy and observe all technical rules, which in any institution should be included in the regulations of institutions for the protection, processing, storage and security of personal data. From the study made in the main institutions of the administration such regulations are lacking. It is to be appreciated the initiative of the authority for data protection, who supports public institutions with *standard regulations in this regard*.

In the case of cooperation with processors, the controller must choose a processor that has such professional skills to meet contractual obligations related to the implementation of technical and organizational security measures. Safety improvement requires the use of technical equipment, which could help to improve safety. While personal data protection intends to protect the personality, data security intends to protect the information, in other words to guarantee, confidentiality, availability; and integrity.

Law no. 9131, dated 09.08.2003 "On the Rules of Ethics in Public Administration" provides in Article 16 for rules regarding the use of information. The provision provides for the obligation of public administration employees even after leaving office, to not use for personal interests confidential information obtained in the performance of the duty. In analogy to the above provision, we may assume that the obligation of public administration employees to maintain confidentiality of the data they control will be extended during the exercise of administrative functions. Maintaining the integrity and availability was emphasized in explaining the principles of data processing by public controllers, although these guarantees are provided only by the law on protection of personal data and not on the legal basis of the functioning of public administration.

Every institution of public administration, *inter alia*, keeps personnel files for its employees, which constitute a special category of data considering the data subjects (personal and professional data of civil servants). The latter, are encountered both as data subjects and controllers within the institution where they engage. However, in this regard data protection is realized with the same security measures, and therefore data will be used in accordance with the special law. We deem it worthy that for meeting the required standards of security of the information developed by public controllers, the latter must meet their goals with the lowest level possible of personal data or if possible to avoid the collection of this category of information and considering, in any administrative process, alternatives that do not require personal data.

5. Data subject's rights

The personal data protection can be analyzed on two levels: firstly, in terms of the active dimension of its implementation and in its passive dimension. The active side of the protection of personal data and information obtained from them is regarded as a right to informational self-determination or the frame of information on private life. This right is based on the presumption that personal data have as their titular only the data subject, from which is derived the right to decide for

themselves on any disclosure or distribution of data for any purpose. In this way, data can be collected and processed with the consent of the data subject, who at the same time exercises the right to control in the event of data processing, by being informed first on the time, on the controller and on the purpose of the processing. The passive dimension of data protection is related to the conditions highlighted in the legislation on the collection and processing of data by the controller, thus forming an actual system of guarantees related to the purpose of data processing (*see above*).

Essentially, the personal data protection represents a subjective right of the category of absolute rights, which vests with obligations any other subject from the category of data controllers to refrain from any abuse with data while processing them and prohibition of their processing when necessary. Data processing by public administration institutions is also subjected to these prohibitions, although any data collection is carried out on the basis of procedures which shall not contravene the general principles mentioned above. Any data gathering by the public authorities should be guided by the real need for fulfillment of their legal duties. Therefore these bodies are obliged to destroy the data when the need for them no longer exists, except when there is a deadline for archiving data specified in a legal act. Meanwhile, if a public administration body systematically collects data, it is obliged to communicate to subjects involved the elements, the purpose of processing data, the legal basis for processing, categories of data recipients, data categories and data recipients. Rights assigned to data subjects to exercise control over their data ensure protection at every stage of processing.

6. The right to access

This means on the one hand, that the data subject has been able to predict that their data will be collected data and that in turn data processing will be done with his knowledge or consent. Based on Article 12 of the Law every person has the right, upon written request, to obtain from the controller confirmation if their personal data are being processed or not, information on the purpose of processing, the categories of data processed and on the recipients and categories of recipients to whom personal data are being disclosed; require in a comprehensible form, personal data and information available on their source and in the cases of automated decisions, under Article 14 of this Law, has the right to request information about the logic involved in the decision. Based on Chapter IV of the Law he has the right to request free information on the data in question, to seek, if necessary, that they be corrected or deleted. Access to information and legislation on data protection are closely linked to the content of the information and it is important that these are treated as cases of limitations when access to information with personal character violates important interests or classified information. The only limitations related to the right to access provided by article 12 of the law are the cases of harming the:

i. National security interests;
ii. Foreign policy;
iii. State's economic and financial interests;
iv. Criminal offences prevention and prosecution.

If the right of access is restricted, these bodies are obliged to inform the applicant of the reasoned decision, in writing, within 30 days. The right to information constitutes the only means for the subject involved, to seek his rights in the area of data protection, thus this right cannot be unlimited, except when absolutely necessary. It is considered a misapplication of this principle when the subject is not acknowledged or has been incorrectly informed about the purpose and type of processing or, is not acknowledged or has been incorrectly informed about the purpose and type of processing.

The law does not define specifically how access is rendered. One possible way is that the data subject be given a copy of the data. Another way is that the data subject be given the possibility to see the data etc. However, it should be made clear that the use of the form is not mandatory and that access can be given in any form set out in the request made. In cases where data collection not from the subject, but by other public body who has access and processes these data, it becomes even more important to implement the standard for informing the subject, who differently not only will not be able to exercise control over their data, but at the same time there will be no opportunity to review the lawfulness of the processing or challenge the processing reasons. We consider that being informed on data processing in the body where they are collected should be extended to any case of transfer of data in other controllers.

Thus, the public controller who collects personal data from another public controller informs the data subject except when the latter is not available or data is collected for the purposes of scientific research and statistics. The law does not provide for deadlines within which, the subject must be informed and the form of providing information. This legal gap could be fixed in cases of completing the package of secondary legislation in public institutions with regard to data

protection (*see above*) and to emphasize the need for training and awareness of public administration on the importance and legal prohibitions in administering personal data to fulfill their responsibilities. When it comes to processing of sensitive data, processing should be carried out with the knowledge of the data subject, unless otherwise provided by law.

To complete the means made available to the data control and protection from their own subject, the legislation provides for the right of objection. Article 15 of the Law provides for this right in cases where data is:

- collected exactly under the focus of this paper for the performance of a legal task of public interest or in the exercise of powers of the controller or a third party to whom the data are disclosed;
- collected for pursuing legitimate interests of the controller or a third party to whom the data are disclosed, except for when these interests prevail on the interests for the protection of the data subject's rights and fundamental freedoms; as well as
- collected for purposes of direct trading;

With this legal mechanism, the data subject asks the controller to not start or, if it has started, to stop processing personal data relating to them. If the requests are justified, controllers must take the necessary actions and inform the individual whether or not an action was taken. If the controller does not fulfill the request of the individual, then he is entitled to exercise their right to appeal.

7. The right to data deletion

This right is linked to the protection of data after data processing for specified purposes and needs of institutions, which should delete or archive data when no longer needed. The right of the individual is exercised to seek correction or deletion of data when acknowledged that data about them are not just and true, are incomplete or are processed and collected in violation of the provisions of the law. The request can be made in writing or orally by a note of the data controller. This request of the individual should be reviewed by the controller and if he is convinced that the claimant is right he shall correct or delete incorrect data.

Pursuant to article 19 of the law, the legislator has concluded the regulation of the right to delete personal data when it appears necessary, not only in the context of the exercise of the right, but more importantly in the obligations the public controller must specifically meet. During the processing of personal data of data subjects, the controller is obliged to perform self-correction or deletion of personal data, when he notes that data are irregular, incorrect, incomplete, or have been processed contrary to the provisions of the law on personal data protection. Not only that, but the legislator has guaranteed that even when the data subject finds that his data is processed illegally, are false or have been processed in violation of the law, he has the right to demand the controller to correct or delete incorrect data. The controller, in conformity with the legal obligation, is obliged to inform the data subject for the performance or non-performance of the correction or deletion, within 30 days. In addition to that, in certain cases the controller shall also inform the recipient of personal data for correction or deletion of personal data transmitted before the correction or deletion. The data recipient in this case could be the processor that has a contract with the controller or any other controller data transmitted to according to the law.

Given the importance of processing incorrect, incomplete data or data processed contrary to the law, we consider that the deadline specified for the controller to answer should be shorter. Experiences of legislation of this field in the region provide for deadlines such as those provided by the Albanian legislator or shorter.

Any person who proves a legitimate interest may request the competent authority to ascertain the illegal character of a data processing, to stop unlawful processing of data, to request the correction, blocking or deletion of data; or to be informed on the data that include them.

Under the current administrative practice, not only the entities involved may submit such claims, but also third parties in certain circumstances in accordance with the Civil Procedures Code.

8. Conclusions

The issue of personal data protection by public controllers - public administration institutions - is part of the core activities of their activity and the fulfillment of public policy objectives, both in the interests of individuals and in the public interest. In any event, the respect of lawfulness and the approach of limited processing should be the only philosophy when operating with this category of information.

In concluding this paper, we ultimately reach to the following conclusions:

1. The need for a secondary legislation framework for data protection in cases of data collection and processing by public administration institutions. This will enable the determination of specific rules for guaranteeing this subjective right regarding the nature of work and powers of the institution;
2. Minimization of data processed by public administration institutions by assessing the need for processing on the basis of the principle of adequacy and its strict implementation. The activity of public administration authorities is considered specific in the administration of data and personal information. Therefore it is considered as more than necessary to establish clear criteria that help even setting a balance between public and private interest.
3. Increased emphasis on the responsibility of the state to prevent infringements that result in violations of personal data and privacy. It considered as more than necessary to establish specific standards for ensuring data security. In the case of public controllers there is a need to define better the individual responsibilities of persons who collect and process data within the institutions and to provide for procedures for their treatment on the importance and legal restrictions in cases of data administration.

Reference

Bennett, C.J. and Raab, C.D. The governance of privacy: policy instruments in global perspective, Surrey: Ashgate Publishing, 2003
Halpern, S. W, "The Law of Defamation, Privacy, Publicity and 'Moral Rights". Cincinnati: Anderson Publishing 1988
Henkin, L., Privacy and Autonomy. Columbia Law Review, 74, 1974, 1410-33.
Hixson, R. F., Privacy in Public Society: Human Rights in Conflict. New York: Oxford University Press, 1987
Daniel J. Solove, Chris Jay Hoofnagle "A model regime of privacy protection", 2006, 42-44
The Universal Declaration on human rights and freedms; The Convention for the Protection of Human Rights and Fundamental Freedoms, amended by Protocol 11, came into force on November 1, 1998;
Directives 2002/58/EC and 95/46/EC of the European Council and European Parliament;
The Council of Europe Convention "For the protection of individuals from the Automatic Processing of Personal Data", ratified by law no. 9288, dated 7.10.2004;
The Additional Protocol to the Council of Europe Convention "For the protection of individuals from Automatic Processing of Personal Data, related to supervisory authorities and cross border movement of personal data" , ratified by Law no. 9287, dated 7.10.2004.
Law no.9131, dated 8.9.2003 "On ethical rules in the public administration"
Law no. 90/2012 "On the organization and functioning of the state administration"
Guidelines on personal data processing in public administration 2013.
Instruction no. 37, dated 10.07. 2013 "On the protection of personal data during the processing of fingerprints by public authorities"
Instruction no. 2, dated 26.07.2010 on "Obligations of data controllers and processors before processing personal data".
Cases ECHR, Leander v. Sweden, 26.03.1987; Kopp v. Switzerland, 25.03.1998; Amann v. Switzerland, 16.02.2000