Protection of Privacy and Personal Data in Albania

Evis Garunja[*]

UDK: 342.738(496.5)
35.083.8:341.231.14(496.5)
34:004.3/.4(496.5)
34:681.3(496.5)
https://doi.org/10.31297/hkju.23.1.3
Original paper / izvorni znanstveni rad
Received / primljeno: 3. 1. 2022.
Accepted / prihvaćeno: 30. 8. 2022.

The protection of universal human rights was accomplished with continuous improvements of both international and domestic laws. Guaranteeing the dignity, the honour and privacy of the persons became values of the civilisation and democracy. Laws provide protection and seek to reduce conflicts and suppress injustices. The paper offers an excursus on the international background and the protection of personal data and privacy as a sensitive issue in international relations. With this regard, Albania is moving forward with improving its legal framework to adapt their quality. Comparative methodology in this research will lead the argument through similarities, differences, and developments of the Albanian society as a part of Europe and part of the technological evolution.

[*] Evis Garunja, Lecturer at the Faculty of Political Sciences and Law, University Aleksander Moisiu, Durres, Albania (predavačica na Fakultetu političkih znanosti i prava Sveučilišta Aleksander Moisiu, Durres, Albanija, email: evigarunja200@yahoo.com).

ORCID: https://orcid.org/0000-0002-2131-3757

Garunja, E. (2023). Protection of Privacy and Personal Data in Albania
HKJU-CCPA, *23*(1), 91–116

Keywords: personal data, privacy, international law, human rights, Albanian legislation, institutional protection

1. Introduction

The protection of universal human rights, the guarantee of dignity, respect for the honour and privacy of the individual are values of civilisation and democracy. Human rights and their birth with national and then international constitutional documents aimed at regulating the relations between the state and the individuals under its jurisdiction. As a part of the human dimension, human rights are essential guarantees of global peace and prosperity. Their concretisation in legal provisions makes them mandatory and essential to suppress injustices and conflicts. The path to achieve these standards for human rights was not easy. The first to be consecrated in the Olympus of inviolable rights were those known as "classical rights" which included the right to life, equality before the law, the right to vote, freedom of expression, freedom of religion, etc. These rights are guaranteed and protected directly by the legal system. The development of these rights is still ongoing. After the World War II, the Universal Declaration of Human Rights of 1948 (UDHR) introduced economic, social and cultural rights (including the right to education, the right to a safe and healthy working environment, the right to housing, the right to social security, health, the right to participate in social and cultural life, etc.) also known as "the second generation of human rights".[1] The rights of "the third generation" came from international legal documents and guarantee the right to peace, the right to protect the environment, the right of the person and his/her family to have necessary standards for development, and the right for a common humanity heritage.

It is this rapid development of communication and information technologies that has forced international/national bodies to adequately assess the full range of effects they produce, not only on socio-economic progress, but also in their guarantees. This has opened the door to the "fourth generation of rights", which are still evolving. The development of the new economy, new techniques for receiving, processing and disseminating in-

[1] The rights of the first generation enshrined in the UDHR and incorporated in Arts. 22-28 of the Universal Declaration and in the International Covenant on Economic, Social and Cultural Rights.

formation and their transfer, has brought about the configuration of the so-called "rights of the technological society". New rights have appeared on the horizon as a result of public relations with citizens, but they have above all emerged due to the advancement of information and communication technologies (ICT) and bioethics.

The emergence of these new rights responds directly to the use and impact of these new technologies in the context of fundamental rights. It is now universally accepted that scientific and technological innovations will influence the future. For this reason, this category of rights is recognised and sanctioned in international documents, constitutions and laws, being identified as categories that allow us to outline the evolution of human rights over time.

These are the new digital rights known as human rights in the Internet age. For example, Internet privacy rights and freedom of expression are extensions of the equal and inalienable rights set out in the United Nations Universal Declaration of Human Rights. According to the UN, "disconnecting people from the Internet violates these rights and goes against international law".[2]

This technological progress has been recognised by the Charter of Fundamental Rights of the European Union – Art. 3 (the right to the integrity of the person) and Art. 8 (protection of personal data) confirm these as fundamental rights in situations arising in the field of bioethics and information technology.

The adoption of the specific EC Directive 95/46, (1995) in accordance with the Council of Europe Convention 108 On the Protection of the Individuals with Regard to Automatic Processing of Personal Data, protects the segment of human rights and fundamental freedoms, protects personal data and privacy. This symbolises the first global step in the institutional protection of personal data and the privacy of the person from abuse and violations by operators and data processors.

Personal data are recognised as personal property only of the person and therefore belong to him/her and only him/her. In its essence, this constitutes personal privacy grouped with one's personal actions. Privacy is defined as a slightly broader term than personal data, and includes the space and environment in which the subject has the right to keep personal data only to him/herself. These data are in principle the foundation of basic human freedoms. Violation, abuse and criminalisation of personal data

[2] https://www.weforum.org/agenda/2015/11/what-are-your-digital-rights-explainer/

through the misuse, mismanagement, abuse and cybercrime by search engines (the Internet, social networks) and the automation of television technology, information technology and digitisation represent a serious threat to the privacy and security of the individual and of the society as a whole, thus undermining national and international security.

2. The Relationship Between Technological Development, Human Rights on Privacy and Personal Data Protection

Technological developments have created excellent structures to promote sustainable economic and social development and the circulation of knowledge, and they profoundly influence the dynamics of democratisation and the promotion of human rights. The Internet is creating new opportunities in the production and exchange of knowledge, becoming an invaluable resource for education, information, research and development of the society. It is also the engine of the global economy, promoter not only of innovation, but also of the main infrastructure for the participation of local businesses in the global economy. As an interpersonal communication platform, the Internet has become the main mean of communication, crossing geographical barriers and establishing a new interaction between public institutions and citizens through the proliferation of mobile devices. This makes the Internet an increasingly necessary tool for social organisation and citizen participation in public matters. With the Internet, virtual or digital rights defined as human rights were born and developed to allow people to access, use, create and publish digital contents or access and use computers, other electronic devices and communication networks.

In addition to meeting the needs of the contemporary society, these inventions pose a challenge for legal systems to guarantee the fundamental rights of the individual. The primary function of the legal order is to minimise the arbitrary exercise of power through well-defined and pre-approved laws. A recent important legal debate on the impartiality of the network has involved the most notable professors of media law, among them Professor Wu of the Columbia University, who defined the Internet service as a public information service (Wu, 2003). According to him, the Internet service is similar to water, gas, telephony, transport service. This debate prompted the American regulator (Federal Communications

Commission) to adopt mandatory rules for the impartiality of the network (2015), with the obligation to Internet service providers and/or the general public not to limit and offer equal treatment to all information, videos, games, comments or any content that was uploaded and / or transmitted online.

In late 2017, the "impartiality of the network" was challenged due to comments from false identities on the Internet favouring free competition and innovation. Considering the regulation of the Internet like any other public service (water or public transport), this led to the slowdown in innovative development and the loss of interest in progress from the leading companies in the field. This raises questions as to whether the new, subjective rights in relation to the development of technology are constitutional rights, and whether a formal update of the human rights catalogue is necessary. Several scholars believe that the use of the Internet has included new subjective situations such as the right to access the Internet (Frosini, 2011) in legal systems. This doctrinal orientation considers the right to access the Internet (Caruso, 2013, p. 9) as a social right (Rodotã, 2010, pp. 337–351), which obliges public authorities to provide the individual with the material means to have access to broadband and fast connectivity (Tozaj, 2017).

On the one hand, innovative inventions help foster the freedom of expression and strengthen competitiveness in the information society (media) sector. On the other hand, the rapid development of technology poses a potential risk for the violation of privacy and personal data. It has been accepted by the doctrine that freedom of expression is not an absolute right. The jurisprudence of the European Court of Human Rights (ECHR) has always interpreted this right in relation to other rights. Among the rights that limit the exercise of freedom of expression, in addition to the right to respect the private and family life, are the following: "the right to a fair trial; property rights; market regulation, media services infrastructure; content adjustments based on different media; adaptations to the journalistic profession; discrimination; the right to life; or the right to organize" (Kasmi, 2018). In the case of Lingens vs. Austria, the ECHR held that in cases where the applicant is a public person, freedom of expression would take precedence over respect for the right to privacy protected by Art. 8 of the European Convention on Human Rights (ECoHR).

The debate on the relationship between the right to information and the right to private life has been raised in recent years to another standard, that of disclosing the personality and identifying the characteristics, pro-

files and preferences of the individual. In this regard, technological inventions such as "Hi Google" or "Hello Alexa" collaborated, thus intruding the privacy of each user. Various advertising platforms are often under attack for manipulating users' wishes. From a "like" or a click to an advertisement on the net, the user ends up flooded with advertisements on the same topic on his/her mobile, PC or personalised pages. Artificial intelligence algorithms are often "scary", as in the case of Google (web browser), which offers us contents we might like and want to see, based on our recent searches.

The use of technology facilitates the direct participation of citizens in the cultural and political life of their country and, more generally, serves as a tool for the emancipation and promotion of fundamental freedoms and the stimulation of the processes of democratisation in the creation of a fair society. The use of the Internet aims to disseminate information in the user's cultural, social, economic and social interactions, which is made possible by media giants such as Facebook, Twitter, Instagram or other networks. Personal data management practices are the bridges of fragile communication between the profitable goal of the media business and the public interest in freedom of expression and the dissemination of information, based on the guarantee of respect for privacy. New technologies have potentially jeopardised the guarantee of the right to work and non-interference in private life. In contrast, Internet distributors (as evidenced by numerous legal practices) process personal data by creating detailed profiles and outlines of the users' personality traits (Kasmi, 2018).

The investigation against Facebook in February 2018 showed the breach of privacy through the use (as claimed) of the personal data of 50 million Facebook users by the British company Cambridge Analytica. This shock has led to a large loss of business on the stock exchange and market volatility[3], as well as drawing the attention of lawmakers around the world towards regulating the use of data by Internet distributors, in order to maintain a balance between profits and public interest. Technological profit must not be at the expense of respect for private life (Kasmi, 2018). Another result of the use of social media pages on the Internet involves the unauthorised use of the users' personal data for the purpose of marketing, electoral or political campaigns. The Facebook scandal opened up a big debate on it.

[3] Only on March 16, 2018, interest in Facebook's stock fell by 6%, resulting in a loss of up to $ 70 billion in one week (https://www.cnbc.com/2018/11/20/facebooks-scandals-in-2018-effect-on-stock.html).

3. The Protection of Personal Data and Privacy

Personal data of the person are an expression of his/her spiritual, material, intellectual and cultural being, the only completely individual and eternal personal property. The violation of these elements is treated not only as a violation of privacy, but also as a violation of the "honour", "dignity" or "personality" of each individual, increasing the degree of sensitivity to the violation suffered. Legally, these rights are defined and regulated by civil law as "personal and non-patrimonial rights", which include: the right to a name, a pseudonym, a residence, copyright, honour, etc. The meaning of the word "personal" shows the connection that this right has with a certain person (Kondili, 2008, p. 99). In constitutional frameworks, as the highest legal acts of the various political systems, the right to privacy occupies a central part. Meanwhile, in secondary legislation, this right is legally regulated through many branches of law, such as civil law, family law, criminal law, inheritance law etc. (Jashari, 2016).

The Universal Declaration of Human Rights, adopted by the United Nations (UN) in 1948 (UDHR, Art. 12) enshrines that "no one shall be subject to arbitrary interference with his/her privacy, family, home or correspondence, nor to attacks on his/her honour and reputation."[4] The text of the Declaration does not refer directly to the protection of personal data, but directs its interpreter to the essence contained in the right to privacy.

UN's International Covenant on Civil and Political Rights, adopted in 1966, establishes the right to privacy in Art. 17 Resolution 68/167 On the Right to Privacy in the Digital Age adopted by the same organisation in 2014, reaffirmed the rights proclaimed in previously mentioned documents. Among other, states were required to respect and protect the right to privacy in electronic communications as well.

Art. 8 of the ECoHR goes beyond Art. 12 of the UDHR, not only as a negative obligation, but also as a positive obligation on behalf of the state. Thus, the state not only does not intervene, but also assumes a positive obligation to protect these rights as realistically as possible through its institutions. Furthermore, the terminological approach in the text of the ECoHR is not the same as the UDHR; the words "honour" and "reputation" are no longer used, they are replaced by the phrase "respect for privacy". Art. 8 of the ECoHR provides the right of every person to seek

[4] This right is presented as a negative obligation on the part of the state not to interfere in people's privacy.

compensation for a violated right before the European Court of Human Rights. The Court has established a practice in this regard through the interpretation of Art. 8 of the ECoHR in the light of the protection of personal data, as an evolved right in compliance with the protection and guarantee of privacy.[5]

The adoption of the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (Convention 108) by the Council of Europe in 1981, and the adoption of the Directive 95/46 on the protection of individuals with regard to the processing of personal data and on the free movement of such data by the European Union aimed at promoting free flow of data. The EU has adopted two other legal instruments in the field of data protection; Directive 2002/58 (e-privacy) for data processing in the electronic communications sector, and Regulation 45/2001 for data processing and free movement between the EU institutions. The EU took an even more important step in the 2000s, affirming the right to data protection as a separate constitutional right (Art. 8 of the Charter of Fundamental Rights of the European Union). European citizens don't have to use the recourse to the right to privacy to protect personal data anymore. Art. 8 of the Charter provides not only the right to the protection of personal data but also the principles of their processing (Cakrani, 2017).

In the field of human rights, the protection of personal data is a part of the catalogue of fundamental rights in the Constitution of the Republic of Albania, Art. 35. Although Albania has given constitutional force to the protection of personal data, the need to approximate existing data protection legislation with that of the EU has paved the way for the adoption of the Protection of Personal Data Act (PPDA) in 2008, in line with the EU Directive No. 95/46.

What is meant by personal data? Various scholars and legal documents have tried to give a broader definition of the terms "data" and "information". Convention 108 (Art. 2) defines personal data as "all information relating to an identified or identifiable person". The EU Directive 95/46 defines personal data as "any information relating to an identified or identifiable natural person" (Art. 2). Even if a single datum cannot be related to a particular person, but there are all the premises and reasons for using

[5] Cases: European Court of Human Rights, Case of Z vs. Finland, Application no. 22009/93, 25 February 1997, European Court of Human Rights, Case of Peck vs. The United Kingdom, Application no. 44647/98, 28 January 2003, European Court of Human Rights, Case of Ll vs. France, Application no. 7508/02; 10 October 2006.

it in combination with other data or information to identify this person, then this is personal data (Schwartz & Solove, 2014, p. 879). In some of their decisions, the European Court of Human Rights and the Court of Justice have based their proceedings on the same definition (Cakrani, 2017).

According to the Albanian Protection of Personal Data Act, "personal data" shall mean any information relating to an identified or identifiable natural person, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his/her physical, physiological, mental, economic, cultural or social identity (Art. 3).

According to this explanation, personal data are related to:

a) any information that provides data on the private and family life of the person, not only information disclosed as a result of his/her continuous activity (school, work, health) or as a result of his personal experiences;

b) a person when it comes to that specific person as it relates to his/her identity, characteristics, behaviour, or whether this information has been used to determine or may influence the way that person is treated or evaluated (in terms of content, purpose and result of the collection of information);

c) identified (person is clearly distinguishable within a group of people) or identifiable (even if the person has not been identified, there are still all the conditions to achieve it) natural person;

d) natural person subject to the law (all citizens of a country, adults, physically and mentally healthy and aware of their obligations towards the state);[6]

e) sensitive data means information that refer to the closest sphere of the person, such as their racial or ethnic origin, political views, union membership, religious or philosophical beliefs, criminal convictions, and health and sex life data. The Albanian Constitutional Court in its decision explains the importance of sensitive data compared to

[6] The European Court of Justice declared that: "There is nothing to prevent Member States from extending the scope of national legislation implementing the provisions of the Directive to areas outside its scope, provided that they do not conflict with other provisions of EU law". European Court of Justice Decision, C-101/2001 of 06.11.2003 (Lindqvist), paragraph 98. ECHR, on its decision on Societe Colas Est case, extended the protection of the private space guaranteed by Art. 8 of the ECHR also to legal persons (European Court of Justice Decision, Case of Société Colas Est and Others v. France, Application no. 37971/97 of 16.4.20202.).

other data, due to their nature and character, and considers them the essence of private and family life.[7] Due to its specific nature, this category of data is subject to special control, processing or consent procedure. Sensitive data are processed only when: 1) consent is granted by the subject, valid for the entire duration of the consent; 2) the processing of data is in the vital interest of the data subject or of another person, even if there is no consent due to mental or physical disability; 3) is authorised in writing by the authority responsible for the processing of sensitive data, in cases of significant public interest; 4) refers to data that are openly public or necessary for the exercise or protection of a legal right; 5) are processed for historical records; 6) there are reasons related to preventive medicine; 7) are processed by political, philosophical, religious or non-profit organisations, trade unionists, for the purposes of their legitimate activity, only to members, sponsors or other persons; 8) processing is necessary for the fulfilment of legal obligations (Art. 7);

f) other personal data includes any type of information belonging to a person, such as court documents. Albanian legislation defines criminal records as "all data relating to sentences in the field of criminal, civil, administrative trials or the documentation in the registers of criminal, civil and administrative convictions" and provides the necessary guarantees for their protection. But what happens when the decisions of the courts are accessible on web pages, where personal data of the people involved in the process are published? If so, does this grant the public's right to information or violate privacy and the protection of personal data? In cases of criminal proceedings against a person of high social risk, the public interest in being informed prevails, as in the case of a person exercising public functions. The situation is more delicate if it is a matter of intimate family or personal disputes, where the publication of personal data will damage the present and the future life of the individual and the whole family even more.

[7] The Albanian Constitutional Court Decision No. 16, of 11.11.2004. para. 4, "Personal data with a patrimonial nature, as a rule, became part of the private life sphere, therefore in this case, the Art. 35 of the Constitution and Art. 8 of the European Convention on Human Rights are applied. However, they do not have the nature and character of sensitive data, which constitute the essence of private and family life."

4. Protection of Personal Data and Privacy in Albanian Law

PPDA recognises the general principle that legal processing of personal data takes place in compliance with guaranteed human rights and fundamental freedoms and, in particular, the right to the protection of privacy. The main rules on which the protection of personal data is based are divided into:

a) *Principles for the protection of personal data*, that are based on their treatment in an honest, correct and lawful way and their collection for specific, clearly defined, legitimate purposes, and whose processing is in compliance with these purposes;

b) *Principles for the processing of personal data.* According to the law, the controller is the person responsible for the implementation of these requirements on all automated or other means of data processing (Art. 5). Their processing is carried out by the official authorities only for the purpose of preventative activities and criminal investigation in the case of a crime against public order (Art. 6/2).

c) *Principles for the transfer of personal data.* The international transfer of personal data is carried out by the recipient from countries with a sufficient level of protection of personal data. The level of protection of personal data for a country is determined by evaluating all the circumstances relating to their processing, nature, purpose and duration, country of origin and final destination, legal acts and security standards in force in the receiving country. In case the level of data protection is lacking, the international transfer is carried out if: a) it is authorised by international acts; b) the interested party has given consent to the international transfer; c) constitutes an obligation for the execution of a contract concluded between the data controller and the data subject or a third party; d) it is a legal obligation of data controller; e) it is necessary for the protection of vital interests of the data subject; f) it is necessary or constitutes a legal requirement for an important public interest or for the exercise and protection of a legal right; g) consists of a register, which is open for consultation (Art. 8). After carrying out the assessment, the data protection commissioner can authorise the transfer of personal data to the host state, establishing conditions and obligations. The commissioner may allow certain categories of international transfers of personal data to a state that does not have a sufficient level of protection of personal data. Before providing the data,

the controller requests authorisation from the commissioner. In the request, the data controller must guarantee the respect of privacy of the data subject outside the Republic of Albania (Art. 9).

PPDA is sensitive in guaranteeing the rights of the interested party, owner of such data, providing the right to obtain information about use or processing of his/her data) (Art. 12); the right to request the rectification or cancellation of data when they are inaccurate, false or incomplete (Art. 3); automatic decision-making to avoid legal effects that can cause automatic data processing (Art. 14); the right of the interested party to oppose to their treatment (Art. 15); the right to complain in case of violation of the rights, freedoms and legitimate interests regarding personal data (Art. 16); compensation for damage deriving from the unlawful processing of personal data (Art. 17). PPDA guarantees measures for the security of personal data (Art. 27). It is the duty of data controller to adopt adequate organisational and technical measures to protect personal data from unlawful destruction, accidental destruction, accidental loss or impediment of access, or dissemination by unauthorised persons, especially in their network.

Only in cases where the data are used to prevent or prosecute a crime can they be processed for a purpose other than that for which the data were collected. The data documentation is kept for the time necessary for the purpose for which it was collected. The level of security should be commensurate with the nature of the processing of personal data. Persons aware of the processed data (owners, data processors, controller, etc.) are obliged to maintain confidentiality and reliability even after ending their function (Art. 28).

Modifications and amendments to the PPDA from 2012 and 2014 were the first to provide the definition of "electronic tools" which include computers, computer programs, electronic or automatic devices that can be used to process data. In contrast to its previous version, this law for the first time defines "direct trade" as communication with any means and any sort of advertising material, using personal data of natural or legal persons, agencies or other units, with or without mediation.

5. The Effects of Technology in the Field of Personal Data and Privacy

As demonstrated above, PPDA provides for the full range of tools used in the collection, processing, and transfer of personal data, whether electronic, mechanical or otherwise, with the sole purpose of protecting and

storing it as fairly as possible. The development of technology has brought on an increase in the threat and risks to the privacy of all, arousing institutional vigilance in assessing the level of potential harm, and undertaking research on the extent of imaginable harm. (Pradel, Corstens & Vermeulen, 2010, p. 403). The invention of the telephone led to the breaking of barriers in the world, from landline telephone to the most advanced telephony models that allow generations to send and receive photographs, written texts, video recordings, films, messages at any distance, through very high-speed voice recording, with the aid of satellite equipment. These devices provide the opportunity for communicators to know and precisely identify their location (addresses) during communication. The ability to know the position during communication, through Google and other sites where the digitised world map is inserted in the GPS system, has allowed the satellite to identify the position and address of the interlocutor. In addition to facilitating human life, technology has created great opportunities for privacy intrusion, because the recipient and the sender on both sides of the receiver obviously record the individual's personal data, and such devices possess the ability to store these records on servers.

The difficult situation of the COVID-19 pandemic has once again highlighted the sensitivity of data protection and the risk that one's actions could from protect the right to life and violate privacy simultaneously. This is how mobile service subscribers in Albania (Vodafone Company, and later AlbTelecom) felt when they heard an audio message from Prime Minister Edi Rama, with "advice" to protect themselves from the corona virus, before calling or receiving a call (March 2020). Every Vodafone subscriber who called any other number to any operator was from time to time forced to listen to an audio message from the prime minister, before connecting to the dialled number. Also, users of any other operator who called a Vodafone number, were occasionally forced to listen to Rama's message before being connected to the dialled Vodafone subscriber. These messages were played randomly, once every few calls. This action was in flagrant violation of ethics, professional standards and the privacy law itself by telephone companies. PPDA allows the use of numbers for preventive medical purposes but requires that such use be made by authorised persons in the health system and public institutions certified for data protection. In this case, the assumptions that would demonstrate that the use of personal data of the subscribers complied with the law did not exist, so the conclusion was simple: the use was made by Vodafone itself, which did not provide the numbers to the Prime Minister's staff, but technically introduced his audio message to subscribers.

The use of the camera as a powerful tool in the process of recording, surveillance and transmission of static and dynamic images has greatly facilitated the increase of surveillance in favour of security and the reduction of the workforce which would otherwise be obliged by their physical presence to monitor certain spaces, maintaining and taking care of the safety of property, people and capital in various situations. Illegal use of camera in spaces such as maternity wards, psychiatric wards, neurology wards, healthcare structures (different sectors), changing rooms (where uniforms are prepared and put on), dressing rooms (in commerce), bedrooms (private areas), etc., would be considered a scandal, and this type of camera surveillance would undoubtedly constitute a serious violation of the rules on personal data protection and privacy.

Individuals have the legal right to be informed about the processing of personal data by means of surveillance cameras. In practice, the information is provided through notices posted in visible and easily accessible points of the space monitored by surveillance cameras. The warning sign contains the clear signal of the camera, the inscription about the observation in the official languages applicable centrally and locally, the space reserved for the data of the controller (such as address, e-mail, telephone, etc.), as well as the logo of the Personal Data Protection Authority. The data controller (person in charge) is not authorised to use camera footage for other purposes than those announced by the Agency, pursuant to the provisions of the PPDA, i.e., if an organisation has announced its intention to install cameras for security reasons, the controller does not have the right to use such images to check the presence or concentration of employees in the workplace.

Although the PPDA provides the application of surveillance with cameras in apartment buildings, the installation of such a system must be subject to compliance criteria with 70% of the residents in favour. In the event that camera surveillance is required for the safety of residents and property, the transmission of the observed space must not exceed the entrance to the structure and common spaces. This action is legitimised upon notification to the Personal Data Protection Authority, as it informs all employees in advance of such action.

Camouflaged cameras are also subject to privacy assessments. No one can use disguised cameras and take over the powers of law enforcement authorities in an attempt to detect illegal activity such as theft without notifying the police. Competent authorities are charged with executive powers to investigate and prosecute these violations. Under normal circumstances, a period of six months is considered sufficient and reasonable to

retain camera surveillance footage. After this time has elapsed, the images should be automatically deleted. In cases where an insurance company holds the images on behalf of the data controller, the controller is obliged to enter a legal agreement with the insurance company which will only act according to the instructions of the controller and in compliance with appropriate technical measures of security against unlawful processing.

The discovery of the radio transmitter (late 18th and early 19th century) paved the way for audio-recording technology which includes processing and transmission over the air (*ether*) of various personal data of public interest and for the general development of society. This involves processing to be carried out in various forms through Dictaphones, such as voice recordings and various conversations of subjects that can be used for transmission or can be kept for proof, whether they are historical, archival, judicial, cultural, security, etc. In this regard, the processing of data of subjects (citizens) in the field of audio recording must be carried out with the consent declared in writing or registered by them (subjects of personal data), guaranteeing the retention of data (where the voice is part of their individuality and therefore deserves respect and protection) and the protection of privacy, as a minimum requirement expressed by the PPDA.

The totality of personal data disclosed in personal documents[8] is used for the identification, free circulation, and legal realisation of citizens' rights during their life, in accordance with the purpose of their registration or collection. State institutions such as police, civil registry, ministry of the interior, consulates, and customs offices are the guarantors of the production, use and security of documents (which must predispose the highest quality on the production and the security of the document's elements) with their biometric data, due to their sensitivity.

The technology for the production of these documents has facilitated free circulation of financial, commercial, administrative, tourist, and various other operations via the Internet on smartphones. The holder of the document, as the legitimate owner, has the right to the data and the means (titles) in which such data are found. Only other persons who might have the similar right are legal guardian, specifically authorised person or legal heir (for children, persons with health disabilities and deceased persons) (Jashari, 2016).

[8] Identity cards, passports, certificates (of birth, death, marriage, residence, citizenship, etc.), driving license, car certificates, student indexes, diplomas, certificates, certificates of alumni, students and citizens, health insurance cards, medical history (anamneses) in public and private hospitals and nursing homes, etc.

Public registers contain a large number of reports/comments/records of data accumulated, derived and created by all public administration institutions, educational institutions, health institutions, land registry and geodesy, security institutions, civil registry institutions, various economic development agencies, various service agencies, judicial institutions, tax institutions, private sector entities, such as financial institutions, enterprises, advocacy services, etc. Much of this data today is computerised, digitised and subject to information technology operations. In order to provide an efficient, quality and fast service under the banner of "e-government", public administration has concentrated a strong information power in its hands.

Albanian Crosscutting Public Administration Reform Strategy 2015-2020 provided alternatives for the functioning of local units as administrative units, including the use of the concept of one-stop shops, which use ICT to provide administrative services at the local level. This is because the administrative units of 61 municipalities operate according to the "one-stop shop" model. Eighty administrative services are provided in these branches through the use of ICT. The support structures (back offices) of the institutions will guarantee the service delivery process under the administration of the Albanian Agency for the Delivery of Integrated Services. Public administration services based on fully or partially digitised systems are: the registration of real estate, the issuance of passports and identity cards, registration and licensing for businesses, etc.

National Agency for Information Society offers some online services and provides information on the e-Albania online platform and many other. The e-Albania portal serves as the single point of contact for government services, 24 hours per day, seven days per week, helping to improve access to information for the general public. The portal is connected to the Government Interaction Platform, which is the basic architecture on which interaction with the electronic systems of public institutions is enabled, and to which 42 institutions that exchange data in real time are connected. So far, information has been published on 170 services provided by the public administration. E-Albania contains many public electronic services, such as access to personal data, company data and the online declaration of personal income.

Electronic media,[9] as a fast communication and marketing tool, have brought to attention the difficulty of maintaining a balance between privacy and communication, falling prey to scandals in the field of privacy

[9] Written press, radio media, audiovisual media, electronic communication multimedia and online media.

protection, (Gutwirth et al., 2012, p. 240). In a hurry to publish the news, it often happens that the rules are violated, and the dignity of the interested party (citizen) is seriously violated in terms of confidentiality of the person and security of his/her personal data, in cases such as revealing photos of begging children, displayed photos/videos of arrested persons, photos of persons handcuffed by the police, photos of people taken in various circumstances without their warning or consent, names and surnames of the defendants (before the judicial process is over), names and surnames of people suffering from contagious diseases, serious illnesses, etc. All these cases constitute violations of the person's privacy and of his/her personal data, and as such are punishable by the relevant law, punishable by the European Directive on the Protection of Personal Data and Privacy, and the European Convention for the Protection of Human Rights and Fundamental Freedoms (Jashari, 2016).

The commissioners and personal data protection authorities have published on their official websites advice and recommendations for the protection of children and Internet users from the possibility of abuse during communication, such as identity theft, change of identity, and publication of abusive images of individuals by various wrongdoers. Opportunities have been provided for the orientation of vulnerable persons towards these mechanisms authorised and mandated by the constitutions and laws on the protection of personal data in the signatory states of Convention 108/1981, adaptation of Directive 95/46, of 1995 and of all aspirant states for EU membership.

6. Final Reflections

Our lives will be increasingly influenced by technological developments, which need a well-defined legal framework and independent institutions, alertness and readiness to take action against the misuse of the technology in order to be kept under control. Despite continued efforts, Albania ranks last in Europe in the Information Technology Development Index for 2016 and ranks 91st out of 175 economies in the world, according to a ranking published by International Telecommunication Union (ITU, 2015). Of the three sub-indexes, Albania ranks best in the one of skills, where it is in 61st place and worst in that of access, where it is in 105th place in the world, while it is at 81st in the index of use (for 2015).

Albanian audio-visual media legislation provides detailed rules for advertising or election campaigns and marketing purposes; however, since tele-

vision has been significantly replaced by social media, new rules are needed on the dissemination of information on the Internet, which emerges from the fact that Albania does not have the means to report harmful information on the Internet, but delegates this task to the General Directorate of the State Police.

Albanian Electronic Communications Act (Law 9918) contains various rules relating to the obligations of operators in the field of human rights protection, including personal data. On the other hand, the Interception of Electronic Communications Act (Law No. 9157) provides some rules that oblige operators to distribute information on the Internet to cooperate with state bodies. Electronic Commerce Act (Law 10128) provides the rules for conducting commercial transactions electronically through the services provided by the information society, for the purpose of protecting participants; legal protection of the privacy of users or their data, as well as guaranteeing the free circulation of information services, is fully aligned with Directive 2000/31 / EC On Certain Legal Aspects of Information Society Services, in Particular Electronic Commerce, in the Internal Market (Directive on electronic commerce). The lack of legal acts has led to poor coordination between the institutions guaranteeing the protection of personal data for Albanian users.

The audio-visual media authority transmits continuous information on the compliance with personal data protection through audio-visual media, but there is still no supervisory authority for online media or online services. Registered business entities are subject to monitoring of compliance with personal data protection by the Commissioner for the Protection of Personal Data. In 2017, the Commissioner issued 22 administrative decisions. Out of these 22 decisions, the subjects voluntarily carried out administrative sanctions in 11 of these cases. In nine decisions, the Commissioner's Office requested judicial enforcement. In the other three cases, the data controllers filed a lawsuit in administrative judicial proceedings. In 2017, 205 complaints were filed with the Office of the Commissioner for the violation of the right to protection of personal data, 38 of which were out of jurisdiction, while 167 were handled under the PPDA. From the administrative inspections conducted at various data processors, it was ascertained that the subject of the complaints is linked to:

– Lack of personal data security (online data processing and online security);
– Unauthorised legal processing of data (dissemination on media and online portals);

– Direct marketing of unsolicited communications, by telephone or e-mail (Kasmi, 2018).

According to the Albanian criminal and civil legislation, the violation of personal data is charged to the interested party. In 2016, 914 cases were concluded for crimes against morality, dignity and the family, as provided by the criminal code, which is 130 more criminal cases than in 2015 (784 criminal cases in 2015, 914 criminal cases in 2016). There were 1,755 claims for damages (Art. 608–654) in 2016. In 2017, 2,968 claims for damages were registered and 1,850 cases concluded.

The Albanian legal framework has no references to personal data belonging to deceased persons or legal entities. Although the categories are not natural persons under the law restrictions, it happens that their data are protected as violation of the privacy and personal data of the natural persons connected to them. The law also lacks the definition of genetic and biometric data.

A review of the list of personal data is required, providing genetic data within the sensitive data category, assuring that the information obtained from them can identify data of a sensitive nature (information on health, origin, etc.). The prohibition of the processing of sensitive data, in principle, has irreversible long-term consequences and is likely to be a precondition for discrimination. This suggests that people's most intimate space will be violated.

Although ECHR case-law has established cutting-edge standards in defining the principles of data collection, storage, purpose or deletion, as well as the measures taken and their adequacy, the challenge of adapting to technological developments is still present (De Hert & Gutwirth, 2009, p. 4).

There is a need for an international global binding act, which would loosen administrative barriers, speeding up and facilitating the process of exchanging information. It is supposed to strengthen the universal character of this right in order to obtain universal recognition of the necessary principles governing the processing of personal data with respect to legal, political, economic and cultural diversity. The right to respect of private and family life reflects an individualistic component: this power consists in preventing the intrusion of others into private and family life (Rodotã, 2009, p. 80). Their protection is not left to the interested parties, but to a responsible and permanent public body. This act is also supposed to resolve the tension between fundamental rights; freedom of expression, the right to information and the protection of personal data should be

sought in the restrictions of these rights. Blocking access to data is not a solution, but policies that allow the use of personal data for specific purposes. The dissemination of strictly personal information is not a public interest, but those relating to public entities and public functions have a legitimate interest.

The right to be forgotten (the right to delete all or part of personal information from the Internet) should teach the Internet to forget, serving to create a selective memory in respect of fundamental human rights but always subject to the freedom of the press to report events, as this constitutes important public objectives. Finding adequate measures to protect public security and the fight against crime and terrorism is an important institutional task.

7. Conclusion

The paper provides basic knowledge about human rights and their correlation with technological developments, being oriented towards social awareness of their importance and the legal standards of personal data protection. The interaction between individuals and state institutions contributes to the recognition of personal data as an integral part of universal human rights. The protection of personal data and their security constitutes an important challenge for the responsible institutions, as well as the affected individual. The need for legal guarantee of the protection of personal data by creating supervisory and monitoring institutions which realise their protection, the institutional ways that guarantee the standards, and the legal consequences in cases of this violation constitute the main axis of the paper.

Reality shows that fundamental rights and freedoms are endangered as a result of the abuse of personal data. The restriction of individual freedoms fosters insecurity and hinders the development of universal rights and democracy in a country. Central state institutions and supervisory institutions for the protection of personal data, as well as public and private bodies that process data, have the obligation to guarantee their protection by avoiding cases of their misuse, as in the case of the wiretapping scandal in Albania in May 2016.[10]

[10] Merkel was asked about the wiretapping scandal in Albania, see: https://tvklan.al/merkel-pyetet-per-pergjimet-ne-shqiperi/

The potential risk of cyber violence crosses state borders and poses a serious threat not only to the individual, but also to the state. This highlights the necessity of greater cooperation between law enforcement institutions that deal with threats that cross borders separately, "encouraging emancipatory measures as preventive acts of the concept of political security" (Collins, 2013, p. 455). In legislation of the protection of personal data, the adoption of specific administrative measures with a restrictive character will positively affect the prevention of abuse and misuse through data administration and processing. The well-defined legal framework on video surveillance with cameras in Albania should better specify the responsibilities, use, security, rights, and obligations of the involved subjects on the use of personal data. The creation of a legal basis that clearly defines the storage terms of personal data would create another standard of protection. The security of database can be realised through the functioning of Information Security Management Standard (ISMS) and the certification of IT experts.

The efficiency of the judiciary system and strengthening of its capacities in terms of the harmonisation with and application of the ECJ standards is of utmost importance. Completing the legal framework with regulations for the protection of personal data from the use of drones by the media is necessary. Any kind of abuse of sensitive data should be treated as a criminal offense and regulated by the personal data protection law, guaranteeing compensation to victims from abusers of their personal data. It is also necessary to increase the influence of international mechanisms and authorities on the security and protection of personal data at national level and apply adequate measures to global communication networks, in order to determine the time limits for the storage of personal data of citizens' profiles, which can currently be found on Google and other networks' profiles without any rules and time limits for their use.

References

Cakrani, E. (2017). *Mbrojtja e te dhenave personale* [*Protection of personal data*] [doctoral disertation]. University of Tirana.

Caruso, C. (2013). The individual on the net: The person's right in Internet time). In G. M. Teruel Lozano, A. Perez Miras & E. C. Raffiotta (Eds.), *Sfide per i diritti della persona dinanzi al XXI secolo: internet e nuove tecnologie*. Madrid, Spain: Thomson Reuters Aranzadi.

Collins, A. (2013). *Contemporary security studies*. Oxford University Press.

Gutwirth, G., Leenes, R., De Hert, P., & Poullet, Y. (2012). *European data protection: In good health?* Dordrecht, Netherlands: Springer, https://doi.org/10.1007/978-94-007-2903-2

International Telecommunication Union (2015). *Measuring the Information Society Report*. Retrieved from https://www.itu.int/dms_pub/itu-d/opb/ind/D-IND-ICTOI-2015-SUM-PDF-E.pdf

Jashari, R. (2016). *Mbrojtja e të dhënave personale, Rast studimor: Republika e Kosovës, Dizertacion për mbrojtjen* [*Protection of personal data, case study: The Republic of Kosovo*] [doctoral disertation]. European University of Tirana.

Kasmi, B. (2018). Zhvillimi i teknologjisë dhe mbrojtja e të dhënave personale [The development of the technology and the protection of personal data] *Revista Avokatia 28*.

Kondili, V. (2008). *E drejta Civile II, Pjesa e posaçme, pronësia të drejtat reale të përkohshme dhe trashëgimia* [*Civil right II, special section, temporary real property ownership and inheritance*]. Tirana, Albania: Geer.

Pradel, J., Corstens, G., & Vermeulen, G. (2009). *Droit pénal européen* [*European Criminal Law*]. Paris, France: Dalloz

Rodotã, S. (2010). Una costituzione per internet [A constitution for internet]. *Politica del diritto, 2010*(3), 337-352, https://doi.org/10.1437/32850.

Rodotã, S. (2009). Data protection as a fundamental right. In S. Gutwirth, Y. Poullet, P. De Hert, C. de Terwangne & S. Nouwt (Eds.), *Reinventing Data Protection?* Dordeecht, Netherlands: Springer, https://doi.org/10.1007/978-1-4020-9498-9_3

Schwartz, P. M., & Solove, D. J. (2014). Reconciling personal information in the U.S. and European, *California Law Review, 102*(4), 877-916, https://doi.org/10.2139/ssrn.2271442

Wu, T. (2003). Network neutrality, broadband discrimination. *Journal of Telecommunications and High Technology Law 2*, 141.

Tozaj, L. (2017). *The human rights in relation to the scientific and technologic developments on the global society* [doctoral disertation]. Universiy of Tirana.

Legal Sources

Charter Of Fundamental Rights Of The European Union, Official Journal of the European Communities (2000/C 364/01)

Convention 108 by the Council of Europe – Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data Strasbourg, ETS -108, 28.I.1981, https://rm.coe.int/1680078b37

Convention for the Protection of Human Rights and Fundamental Freedoms, Rome, 4.XI.1950

Directive 95/46/EC of European Parliament and European Council, October 24, 1995, "On the protection of individuals with regard to the processing of personal data and on the free movement of such data", OJ L 281, 23.11.1995

Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning "The processing of personal data and the protection of privacy in the electronic communications sector" (Directive on privacy and electronic communications), OJ L 201, 31.7.2002

Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), OJ L 201, 31.7.2002

Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, OJ L 119, 4.5.2016

Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 On certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce'), OJ L 178, 17.7.2000

Personal Data Protection Act 2008, https://www.informatica-juridica.com/anexos/personal-data-protection-act-2008/#:~:text=(1)%20The%20aim%20of%20this,to%20inviolability%20of%20private%20life

Law No. 8417, dated 21.10.1998 "Constitution of the Republic of Albania" Amending Law no 9675, dated 13.1.2007, Amending Law no 9904, dated 21.4.2008, Amending law no 88/2012, dated 18.09.2012, Amending law no.137/2015, dated 17.12.2015

Law No. 9918, dated 19.5.2008 "Albanian Electronic Communications Act" (updated with the law no. 102/2012, dated 24.10.2012, nr. 107/2018, dated 20.12.2018; nr. 92/2019, dated 18.12.2019)

Law 9157 dated 04.12.2003 "On the interception of electronic communications" (updated with the law no.9885, date 3.3.2008) (updated with the law no.10 172, dated 22.10.2009) (updated with the law no.116, dated 13.12.2012) (updated with the law no. 69, dated 27.4.2017) updated the title with the law no. 116, dated 13.12.1012

Law 10128 dated 11.5.2009 "On electronic commerce" updated with the law no. 135/2013 "For some changes on the law no. 10128, dated 11.5.2009 "On electronic commerce"

Law no. 9887 dated 10.03.2008 "On the protection of personal data" updated with the law no. 48/2012, updated with the law no. 120/2014 "On the protection of personal data"

Resolution 68/167, "The right to privacy in the digital age", UN General Assembly, 2014

Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 On the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and

on the free movement of such data, Official Journal L 008, 12/01/2001 P. 0001 – 0022

Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on "The protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data", OJ L 8, 12.1.2001

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 On the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ L 119, 4.5.2016

The International Covenant on Civil and Political Rights, Adopted and opened for signature, ratification and accession by General Assembly resolution 2200A (XXI) of 16 December 1966

Judical Decisions

European Court of Human Rights, Case of Z vs. Finland, Application no. 22009/93, 25 February 1997.

European Court of Human Rights, Case of Peck vs. The United Kingdom, Application no. 44647/98, 28 January 2003.

European Court of Human Rights, Case of Ll vs. France, Application no. 7508/02; 10 October 2006.

European Court of Human Rights, Case Rotaru vs. Rumania, Application No. 28341/954, 04 May 2000,

European Court of Human Rights, Aman vs. Switzerland, Application No. 27798/95, 16 February 2000,

European Court of Human Rights, Case of Societe Colas Est and Others vs. France Application no. 37971/97, 16 April 2022,

European Court of Justice, Decision, Lindqvist, C-101/2001 of 06.11.2003

Albanian Constitutional Court, Decision No. 16, 11.11.2004

PROTECTION OF PRIVACY AND PERSONAL DATA IN ALBANIA

Summary

The Protection of Personal Data became an important issue for the Albanian citizens. The new era of the protection of personal data through administrative claims started after 2008. This brought up sensitive issues like unauthorised legal processing of data on media and online portals, e-mail lack of personal data security, online data processing and online security etc. The sensibility of people increased when personal data were used for political or commercial benefits. During the COVID-19 pandemic period our lives were dominated by technology as the only means of connecting with others or continuing our normal life in abnormal conditions. On one side, human rights were suffering the most powerful restrictions and on the other, technology was gaining position faster. This paper raises questions on the relation between the protection of dignity, honour and privacy of the persons as a democratic value and technological evolution. This paper aims to introduce the Albanian legislation on the protection of privacy and personal data, legal reforms and their adaptation to international law through case law and jurisprudence. Findings, suggest the need for an international global binding act, which would facilitate the process of exchanging information, reduce administrative barriers, and increase the connection and collaboration.

Keywords: *personal data, privacy, international law, human rights, Albanian legislation, institutional protection*

Garunja, E. (2023). Protection of Privacy and Personal Data in Albania
HKJU-CCPA, *23*(1), 91–116

ZAŠTITA PRIVATNOSTI I OSOBNIH PODATAKA U ALBANIJI

Sažetak

Zaštita osobnih podataka za građane Albanije postalo je važno pitanje. Nova era njihove zaštite putem upravnih mjera započela je nakon 2008. kada se osjetljivost ovih pitanja pokazala u neovlaštenom korištenju osobnih podataka u medijima i nedostacima u sigurnosti osobnih podataka u e-mail komunikaciji te online okruženju. Osjetljivost je posebno porasla kada su osobni podaci bili korišteni za političke ili komercijalne probitke. Tijekom pandemije COVID-19 ljudski životi postali su još i više uvjetovani tehnologijom kao ponekad jedinim načinom povezivanja, odnosno nastavljanja normalnog života uslijed ne tako normalnih okolnosti. S jedne strane, ljudska prava pretrpjela su velika ograničenja, dok je s druge strane tehnologija sveudilj jačala svoju poziciju. U radu se propituje veza između zaštite dostojanstva, časti i privatnosti kao demokratskih vrijednosti s jedne i tehnološke evolucije s druge strane. Namjera je predstaviti albansko zakonodavstvo o privatnosti i zaštiti osobnih podataka, zakonodavne reforme i prilagodbu domaćeg pravnog okvira relevatnom međunarodnom pravu i jurisprudenciji. Nalazi ukazuju na potrebu za postojanjem međunarodnog globalno važećeg pravnog dokumenta koji bi olakšao proces razmjene informacija, smanjio administrativne zapreke te ojačao povezivanje i suradnju.

Ključne riječi: *osobni podaci, privatnost, međunarodno pravo, ljudska prava, albansko zakonodavtsvo, institucionalna zaštita*