SIPARUNTON
International Journal of
Interdisciplinary Research

ISSN 2337-0556 (Print)
ISSN 2337-0572 (Online)
Vol 1, Issue 5, October 2015

==========

Interception of communications for criminal purposes in Albania and compliance with European Union standards

Evisa Kambellari

Faculty of Law, University of Tirana, Albania
E-mail: evisa.kambellari@fdut.edu.al

Brunilda Bara

Head of the Judicial and Documentation Department, Constitutional Court, Albania
Email: bruna.bara@gjk.gov.al

Abstract

This paper makes an outline of the main safeguards elaborated at European level in addressing cases of interferences made by public authorities into private communications for the purposes of crime prevention and the protection of public order. The aim is to confront the European standards on the subject matter with the respective regulation in the Albanian legal framework and practice, and the compliance of the domestic approach with the recommendations of the European Community.

Interception techniques have been used since the invention of the first distant communication means, providing useful information in criminal investigations. The intercepted data play a crucial role on crime prevention, protection of national security and discovery of the truth in criminal matters. However, the means used in the fight against crime must be in line with, protect and not contradict the fundamental values of a democratic society. Such interference should be justified not only in terms of its legal grounds but also in terms of its legitimacy. In this respect, the paper provides an insight into the relevant legal reasoning of the European Court of Human Rights on such matters, identifying case by case whether

==========

there has been an interference in the right of the secrecy of communications; if the interference was in accordance with the law; if it pursued a legitimate aim; and whether it was necessary in a democratic society.

Further, the paper addresses problems noted in the Albanian legislation on interceptions and provides recommendations on the necessary amendments that would ensure individual's fundamental rights and freedoms against arbitrary use of state power, through secret surveillance measures. The main thematic issues and views are addressed by making constant reference to the relevant case law of the ECtHR and European Court of Justice. Special attention is paid to the fact that the Albanian High Court (AHC) does not have a clear standpoint regarding the legal value of interception results obtained using secret surveillance measures. Inconsistencies and double standards in the Unifying Practice of AHC, when referring to relevant ECtHR case law, constitute an additional argument for supporting the national judicial decisions.

The paper tries to present, through ECtHR case law and interpretations, its approach on the subject matter and the set of surrounding circumstances in which they might be applied.

Finally, the paper focuses on the regime provided under the EU Data Retention Directive (2006/24/EC) regarding retention of communications traffic data for criminal purposes and its impact in the Albanian law on electronic communications. Several questions are raised on the future of domestic regulations on this matter, considering that the Directive has been declared invalid by the Court of Justice of the European Union.

Keywords: *Albania, communications, case law, European Union safeguards, interception*

1. Introduction

In the normative structure of the European Union confidentiality of communications is guaranteed in accordance with international human rights instruments, through the provisions of the European Convention for the Protection of Human Rights and Fundamental Freedoms and the Charter of Fundamental Rights of the EU. The first point of reference is the Council of Europe's Convention on the Protection of Human Rights and Fundamental Freedoms of 1950, Article 8 of which states: "Everyone has the right of respect of his private and family life, his house and correspondence." The Charter of Fundamental Rights of the European Union (EU), announced in December 2000, also contains specific previsions on the

right to respect for private life. Article 7 of the Charter provides the right of every citizen "to respect for his private and family life, home and communications".

Meanwhile, the main text of the reference in the European Community with regard to personal data protection is Directive 95/46/EC. The main purpose of this Directive is the protection of individuals' fundamental rights and freedoms and in particular the right to privacy, related to the processing of personal data. The Directive proves the necessary criteria to be respected by the processing authorities. It provides the obligations for a lawful and fair processing and collection of personal data and, in particular, that the data must be adequate, relevant and not excessive in relation to the purposes for which they are processed;[28] Until 2014, problems related to the retention of traffic data of electronic communications for prosecution purposes, were regulated by Directive 2006/24 of the European Union "On data retention". Nevertheless, such Directive was declared invalid by decision of April the 8-th, 2014 of the Court of Justice of the European Union. Such declaration makes its current status unclear. A memorandum of the European Commission[29] states that *"Even under the invalidity of the Directive, data retention will continue to be allowed in accordance with Directive 2002/58 "On the processing of personal data and protection of privacy in the electronic communications sector".* Such provisions imply that local authorities may continue to require data retention for prosecution purposes, but in the exercise of their powers, they must ensure that storage and further processing of such data respects the requirements for the protection of privacy, in accordance with Directive 2002/58.

2. Standards established by the European Court of Human Rights

It is important that the problems related to interference in personal communications for the purposes of criminal prosecution, be seen under the optics of the European Court of Human Rights, considering the huge impact this Court's jurisprudence has on those member states of the European Union, part of the Convention, and the fact that the European Court of Justice (ECJ) bases its decisions substantially on ECtHR's jurisprudence when deciding on limitation of human rights and fundamental freedoms. It is recognized that ECJ regularly refer to the ECHR and the ECtHR's case law when adjudicating on fundamental rights in Community law, having the ECHR its primary source of inspiration. Therefore, the ECJ's

[28] Article 28 of Directive 95/46/EC "On the protection of individuals with regard to the processing of personal data and on the free movement of such data".
[29] European Commission Memorandum no. 14/269, *'Frequently Asked Questions: The Data Retention Directive.'* Brussels, April 8, 2014.

interpretations of fundamental rights in Community law will usually be parallel to that of a similar Convention right by the ECtHR (Lock, 2009, 380).

When deciding on a complaint made by an individual on violation, by state authorities, of his right to privacy of correspondence, ECtHR evaluates three criteria; if the interference is (i) in accordance with law; (ii) necessary in a democratic society; and (iii) in furtherance of a legitimate aim identifi ed in Article 8 (2) (Marshall, 2009, 39).

2.1 Is the interference in accordance with the law?

In order to be in accordance with the law, the interference must have its legal basis on the provisions of domestic law.[30] ECtHR has stated that the term "law" will be evaluated according to the interpretation made by the state issuing the norm, but in any case it should be evaluated if the law meets the three key requirements relating to: (1) the existence of adequate and effective guarantees against arbitrary interference by state authorities in the recognized rights of the Convention; (2) accessibility to the law of the concerned parties, and (3) the clarity and precision of legal provisions.[31] The law should provide at least the minimum guarantees such as: the nature, scope and the duration of the implementation of such measure, the causes that made the measure necessary, the competent authorities for the enactment, implementation and monitoring of these measures and the possible domestic remedies in respect of the alleged violation.[32]

The demand for accessibility (access) to law requires that individuals must be given the opportunity to access the law/ legal provisions that affect them, challenge their contents and moreover be able to foresee the consequences that may derive from the application of the law in question. In *Leander v Sweden*[33], ECtHR stated that an individual cannot be able to foresee precisely what checks will be made in his regard by the special police service in its efforts to protect national security. Nevertheless, in a system applicable to citizens generally, the law has to be sufficiently clear in its terms to give them an adequate indication as to the circumstances in which and the conditions on which the public authorities are empowered to resort to this kind of secret and potentially dangerous interference with private life.

---

[30] *Malone v. United Kingdom*, decision no. 8691/79, dated August 2, 1984; *Kruslin v. France*, decision no.11801 / 85, dated April 24, 1990.

[31] See above *Malone v. United Kingdom*; *Huvig v. France*, decision no. 11105/84, dated April 24, 1990, *Kopp v. Switzerland*, decision no. 13/1997/797/1000, dated 25 March 1998

[32] *Association for European Integration and Human Rights and Ekimdzhiev v. Bulgaria*, decision no. 62540/00, no. 62540/00 June 28, 2007.

[33] *Leander v Sweden*, decision no. 9248/81, dated March 26, 1987, pp 51.

2.2 Does the interference follow a legitimate aim?

According to ECtHR's case law, the obligation to provide the reasons for the interference on the rights guaranteed by Article 8 of the Convention rests with the state authorities that have carried out such interference.

These authorities must argue that the interference was necessary for the protection of: national security, public safety or economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.[34] The measures taken by state authorities interfering with individual's right to correspondence have mostly been justified on grounds of the need for protection of national security and crime prevention. National security means protection of the country from the risks of harm posed by activities of internal and/or external enemies aiming to overthrow the government, or violent attacks against the democratic system. In such cases interception measures become necessary on the fight against terrorist threats or sophisticated forms of espionage.[35]

2.3 Is the interference necessary in a democratic society?

The Court has explained in *Handyside v UK*[36] that the term "necessary" does not mean that the interference is irreplaceable by other means. It means that the interference corresponds to an imperative social need and, in particular, to a legitimate aim pursued by state authorities.

In assessing the existence or not of an imperative social need, state authorities are granted a certain degree of freedom, known as the margin of appreciation.

In *Klass and others v Germany*, the Court stated that *it is indisputable that the existence of legal provisions, authorizing police officers to intercept communications and to secret surveillance, which help them exercise their duties to investigate and discover criminal offenses, can be "necessary in a democratic society for the prevention of disorder and crime".*[37]

However, the Court points out again *that "the exercise of these powers, because of the inevitable secret nature that characterizes them, carries with it the risk of abuse that is potentially easy in individual cases and could have harmful*

[34] *Klass and others v. Germany*, pp 39, "2".
[35] These issues were highlighted for the first time in *Klass and Others v Germany*, decision no. 5029/71 dated September o6, 1978, pp 48.
[36] *Handyside v UK*, decision no. 5493/72, dated December 7, 1976.
[37] *Klass and others v. Germany*, pp 48

consequences for the democratic society as a whole".[38] As a result, the interference will be considered "necessary in a democratic society" if the special system of secret surveillance contains adequate guarantees against abuse.

3. Interception of communications under Albanian law

Articles 221-222 of Albanian Code of Criminal Procedure (ACPC) allow the interception of communications and secret surveillance and the use of such evidence in court. Interception of communications of a person or a telephone number, by telephone, fax, computer or other means of any kind, … and the recording of incoming and outgoing telephone numbers, is permitted only where there is a proceeding for: a) intentionally committed crimes punished by imprisonment of no less than seven years; b) criminal contravention of insult and threat committed by means of telecommunications (Article 221/1).

The court, as provided by law, through a reasoned decision, authorizes prosecutor's request for the interception … *when there is enough evidence for a charge to be filed*. As provided by Article 149 of ACPC, "Evidence is a notice (information) on the facts and circumstances relevant to the criminal offence, which are obtained from sources provided for by the criminal procedural law, in accordance with the rules prescribed by it and which serve to prove or not the commission of the criminal offence, its consequences, the guilt or innocence of the defendant and the extent of his responsibility".[39] Interceptions, carried out according to the provisions of ACPC, constitute a special tool in search of evidence, meaning that the results obtained from such surveillance can be used as evidence in criminal proceedings. Nevertheless, Article 221/5 of ACPC clearly provides that the results of preventive interception cannot be used as evidence.[40] Preventive interception is regulated by a special law.[41] Surveillance methods, applicable by subjects authorized by this law, are not regulated by the provisions of the criminal procedural legislation and the results of preventive interception of communications cannot be used as evidence in trial. The information gathered by this type of interception is used by intelligence structures only in cases of emergency, for the discovery of serious crimes that have been committed or are expected to be

[38] *Handyside v UK*, pp 56

[39] <www.legislationonline.org>, Criminal Codes, Criminal Procedure Code of Albania, accessed 18.05.2015

[40] Results obtained by intelligence services or informative police services in the implementation of their duties for the prevention of crime as provided by the law no. 9157, dated 04.12.2003 "On Interception of Telecommunications".

[41] Law no. 9157, dated 04.12.2003 "On Interception of Telecommunications", amended by Law no. 9885, dated 03.03.2008, and by law no. 116, dated 12.13.2012.

committed. That is because gathering of such information is conducted in such a way that does not offer to the individual the necessary procedural guarantees for the protection of his private life or his other fundamental rights.

Even though, formally, the provision seems clear and does not give rise to different interpretations, in Albania's High Court (AHC) case law of recent years, when determining the connection between the provisions of Article 221/5 and Article 222/1 of ACPC, a double standard can be noticed. Thus, in two of its decisions, based on similar facts and circumstances, AHC reasoned differently. In its decision no.33, dated 13.10.2010, High Court's Criminal Panel abrogated the decisions of the lower courts and rejected Prosecution's request for interception of communications of I.S., J.GJ. and B.M, reasoning that the decisions of the lower courts were held in violation of criminal procedural provisions, namely to Articles 221/5 and 222/1 of ACPC.

According to AHC's Criminal Panel, the courts based their decisions in contradiction to the obligations provided in Article 221/5, mainly on such evidence, which was gathered, as resulted from the information provided to the courts by the Albanian Information Service (AIS), through preventive surveillance. The [lower] courts had considered preventive surveillance as "sufficient evidence to prove/satisfy a criminal charge" (as required by Article 222/1 of the Criminal Procedure Code), even though according Article 221/5 of ACPC use of such evidence is against the law. Furthermore, the Criminal Panel held that both lower courts, in their decisions, considered preventive surveillance's results as "strong and based suspicions". Such evidence, even formally did not amount to sufficient evidence to prove the criminal offence, as required by Article 222/1/b of ACPC when acceding interception of telephone calls and communications. AHC held that the measures taken were unlawful and that the individuals under investigation had limited constitutional rights and freedom, as their surveillance was performed in contradiction with the provisions of ACPC, using as "evidence" acts regarded and used in contradiction with the law and the requirements of Article 149 of ACPC.

Meanwhile, in its decision no.129, dated 12.10.2011, High Court's Criminal Panel held that *"AIS's information, information from foreign services and other operational data, satisfy court's subjective assessment on "sufficient evidence" to prove the criminal charge, because at the time the interception was authorized, there was no culpability of the individual - holder of the telephone number being intercepted.*

On June 2014, the Council of Ministers of the Republic of Albania enacted decision no.354 "On the establishment of IMEI databases for the registration of IMEI numbers of mobile phones, used in mobile network communication services" which entailed the obligation of Albanian citizens to register their IMEI numbers.

Such decision of the Council of Ministers was opposed by a group of members of the Albanian Parliament, who filed a complaint with the Constitutional Court regarding constitutionality of the decision, arguing that even ECJ, by its judgment of 8 April 2014 on joined cases C-293/12 and C-594/12, declared invalid Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and its amending Directive 2002/58/EC. After the constitutional complaint was filed, on 1-st of October 2014, the Council of Ministers enacted decision no.642, which declared invalid the previous decision no.354. The Constitutional Court of Albania, by its decision no.57, dated 05.12.2014 ceased the case.

3.1 Preventive interception

Albanian Criminal Procedure Code holds no provisions regarding preventive interception, as a form of interception carried out by informative state institutions, established by law, for the fulfillment of their duties. Preventive interception aims to increase the effectiveness of the work against dangerous criminal activities and the prevention of possible consequences that may occur. Such interception is regulated by a separate law "On Interception of Electronic Communications"[42]. Considering the sensitive nature of different aspects of private life which may be affected by the interception, the legislator in this law tries to make clear the rights and obligations of the parties involved, to define the principles that should guide them when performing their duties and the requirement for certain criteria to be met, which allow interception. Despite lawmaker's efforts for full and clear amendments to the law on the procedures for performing preventive surveillance, and legislator's intentions to create the necessary control mechanisms to prevent abuse of power, the result achieved appears to be insufficient to meet these goals. There are still issues that require further amendments and possible review by the legislator.

Thus, the explanation of the concept "individual/subject under surveillance" remains unclear, giving rise to subjective interpretations.

Article 3, paragraph 8 of the law states: "Are subject to interception the individuals suspected as perpetrators of serious crimes". Meanwhile, none of the provisions of the law defines which criminal offences will be considered as serious and that could justify the interception of communications of a person based on the suspicion of him being the author of a crime.

[42] Ibid, law no. 9157.

Such a solution seems to be in contradiction with the orientations given by the European Court of Human Rights regarding the criteria to be met by laws on secret surveillance, against any arbitrary interference with the right to confidentiality of communications.

The Court has emphasized that in assessing whether the interference violates or not such right, it must be assessed not only whether the actions carried out by state authorities were in accordance to the legal provisions, but also *the law is sufficiently clear in its terms to give the individuals adequate indications as to the circumstances in which and the conditions on which the public authorities are empowered to resort to secret and potentially dangerous interference with private life.*[43]

This is also known as the requirement for foreseeability and the demand to respect it is directly connected to the guarantees for the protection of legal certainty.

Moreover, in the case of *Contreras v Spain*, the Court held that a law authorizing secret surveillance of communications will be considered that provides the necessary guarantees against interference in individual's private life if it provides, inter alia, the nature of crimes for which such surveillance is permitted.

The expression "serious crime" used in law "On Electronic Communications Interception" is not clear enough to understand the nature of the crimes for which interception may be permitted.

Lack of legal reasons for interception can give rise to abuse of power. Several questions arise. When implementing this law "serious crimes" will be considered only the ones committed against constitutional order and state's democratic institutions? Or those that severely infringe public order and security, such as acts committed by criminal organizations? Will other crimes, such as those that seriously infringe individual's fundamental rights and freedoms, be considered serious or those committed by employees of police structures?

The answers to these questions become even more important especially after the changes the law has undergone, which provide that preventive surveillance can also be required by police officers and Internal State Control Services.[44]

4. Data retention for investigation purposes

[43] *Leander v. Sweden*, decision no. 9248/81, dated March 26, 1987, pp 51.

[44] Internal Control Service is a department of the Ministry of Internal Affairs, responsible for the prevention, detection and documentation of criminal activity, carried out by employees of State Police and other structures of the Ministry of Internal Affairs. (Article 2 of the law no.8748, dated 01.03.2001 "On Internal Control Service").

External data of communication allow the collection of traces of evidence that contribute to the reconstruction of a criminal event. Thanks to them other information on the activities and connections between individuals suspected of committing a criminal offense and the victims can be detected and put to further verifications.[45]

According to provisions of the law no. 9918, dated 19.05.2008 "On electronic communications in the Republic of Albania", the providers of networks and public electronic communications services are obliged to store and administer, for a period of 2 years, data files of their subscribers or users.

Information required to be stored is primarily related to data needed for:

- Identification of the subscribers;
- Identification of terminal device used during the communication;
- Detection of the location and identification of communication's source;
- Detection of the location and identification of communication's destination;
- Identification of the date, time and duration of communication;
- Identification of the type of communication;[46]

In no case such data relates to the content of communication and the storage

[45] Ibid.

[46] According to Article 101, files should contain data regarding ***voice communication and SMS / MMS***, which allow:

a) identification of subscribers, by ensuring the collection and recording of their full identity;

b) identification of terminal equipment used during communications;

c) detection of the location, date, time, duration of communications, caller ID and dialed number, including data on unanswered calls.

3. Regarding cases of ***Internet communications***, the file must contain:

a) the necessary information for tracking and identification of the source / origin of communication:

i) subscriber's identity (user ID);

ii) subscriber's identity (user ID) and phone number assigned to communications that enter in the public telephone network;

iii) the name and address of the subscriber or registered user to whom is assigned an IP address, user ID (user ID), or a phone number assigned during communication;

b) necessary data to identify the destination of the communication;

i) in the case of internet telephony, user ID (user ID) or phone number of dialed number;

ii) in the case of electronic mail or internet telephony, the name and address of the subscriber or registered user and the user's identity of (user ID) the intended communications recipient;

c) ***necessary data to identify the date, time and duration of the communication:***

i) the date and time of connection (log in) and termination of (log off) access in the internet service, according to the local time;

process is different from interception of communications.

However, the collection of traffic and location data can seriously violate the right to private life. Altogether they allow for very precise conclusions to be reached, regarding individuals private life such as everyday life habits, places of permanent or temporary residence, their daily movements, activities performed, social relationships and social environments frequented by them.[47]

Law "On electronic communications" states that data files are stored in accordance with the legislation on personal data protection. Through this provision the legislator provided only the standards applicable to the process of data storage while such data are held by service providers, but did not make any reference to the procedures to be followed such data is made available to relevant authorities.

The law is also unclear regarding the subjects authorized to access and use data files and under which conditions they can gain access for prosecution purposes. Article 101/6 provides that data files are made available without delay, upon request, to the authorities provided in ACPC.

Meanwhile, ACPC clearly provides when interception of communications is permitted and the entities authorized to intercept, nevertheless it contains no provision regarding storage of communication data traffic. Because such data does not provide the content of the communications the laws applicable to interception cannot be used to such data as the storage process is different from interception. Moreover, the interception of communications of a person according to ACPC is helpful tool in search of the evidence and can be authorized by the court if necessary to continue an investigation started and if there is sufficient evidence for a criminal charge to be filed.

Collection of traffic communications data is useful tool not only during a criminal investigation, but also before the investigation is started, that enables the collection of information for the prevention of a crime or to ascertain necessary facts for the initiation of criminal proceedings. Given the different natures between traffic data storage and interception, and the different circumstances for their implementation, Albanian law remains unclear which entities can request storage of such data.

Albanian current legislation on data storage follows the rules set by Directive 2006/24 of the European Union "On data protection". This Directive aims

ii) IP address, determining whether is dynamic or static, as assigned by the Internet service provider;
iii) the identity of the subscriber or registered user to access Internet services.
* The term 'user ID' means a unique identification number assigned to a person the moment he agrees or is enters/enrolls in an Internet access or communications service.
[47] Decision dated April 8, 2014 the European Court of Justice, paragraph 27.

to harmonize the legal framework of EU Member States concerning obligations and duties of networks' service providers and services of public electronic communications on storage of specific external data communications, for the purposes of investigation, detection of criminal offences and prosecution of criminal offenders by prosecution authorities, as provided by domestic laws of member states.

This Directive, in its current form was declared invalid by the Court of Justice of the European Union (CJEU) as it interfered with individual's right for private and family life and the right for personal data protection. In its decision of 8 April, 2014,[48] CJEU held that retention of data as provided by such Directive constituted an impermissibly broad and serious interference with fundamental human's right to private life and personal data protection. As such, the Directive was considered incompatible with Articles 7 (right to respect private and family life) and 8 (right to protection of personal data) of EU's Charter of Fundamental Rights.

CJEU held that: "By requiring the retention of the data listed in Article 5(1) of Directive 2006/24 and by allowing the competent national authorities to access those data, Directive 2006/24, as the Advocate General has pointed out, in particular, in paragraphs 39 and 40 of his Opinion, derogates from the system of protection of the right to privacy established by Directives 95/46 and 2002/58 with regard to the processing of personal data in the electronic communications sector, directives which provided for the confidentiality of communications and of traffic data as well as the obligation to erase or make those data anonymous where they are no longer needed for the purpose of the transmission of a communication, unless they are necessary for billing purposes and only for as long as so necessary.[49]

It follows from the above that Directive 2006/24 does not lay down clear and precise rules governing the extent of the interference with the fundamental rights enshrined in Articles 7 and 8 of the Charter. It must therefore be held that Directive 2006/24 entails a wide-ranging and particularly serious interference with those fundamental rights in the legal order of the EU, without such an interference being precisely circumscribed by provisions to ensure that it is actually limited to what is strictly necessary.[50]

Moreover, whilst seeking to contribute to the fight against serious crime, Directive 2006/24 does not require any relationship between the data whose retention is provided for and a threat to public security and, in particular, it is not

[48] Judgment of ECJ (Grand Chamber) of 8 April 2014 in joined cases C 293/12 and C 594/12 <http://curia.europa.eu/juris/document/document.jsf?docid=150642&doclang=EN>, accessed (May 14, 2015)
[49] Ibid, pp 32
[50] Ibid, pp 65

restricted to a retention in relation (i) to data pertaining to a particular time period and/or a particular geographical zone and/or to a circle of particular persons likely to be involved, in one way or another, in a serious crime, or (ii) to persons who could, for other reasons, contribute, by the retention of their data, to the prevention, detection or prosecution of serious offences.[51]

Conclusions

For the protection of legal certainty, as an important aspect of the rule of law, Albania's High Court must pay more attention to its decision making process and should show consistency in its decisions when dealing with cases of interference by state intelligence authorities to individual's right for protection of personal data, as an important aspect of his right to private life. At present, this Court's reasoning on the protection of such data, according to European standards as set by ECtHR case law, remains vague and opened to different interpretations, creating double standards and giving room to arbitrary use of power by state authorities.

Albanian law no. 9157 "On the interception of electronic communications" needs further reviewing, in order to properly define and give a clear definition of the term "subject under surveillance". The law should also provide the categories of offenses to which preventive surveillance measures can apply. In its current conditions, this law does not fully meet the standards established by ECtHR case law concerning cases of interception of communications.

Bearing in mind that law no. 9918 "On electronic communications" follows the standards set by EU's 2006/24 Directive on data storage for prosecution purposes, the problems related to the implementation of this Directive are also present in Albania's respective law. In this sense, it is necessary to consider the possibility of a revision of the law in order to achieve an approach which best guarantees individual's right to privacy and protection of personal data, in accordance with the standards established in international instruments and domestic laws that specifically protect such rights. The decision issued by the European Court of Justice should be taken as a landmark in assessing current problems that the European model, used for the enactment and the implementation of Albanian law on data retention for prosecution purposes, presents.

References

[51] Ibid, pp 59

Books and articles

- Marshall, Jim. *Personal Freedom through Human Rights Law? Autonomy, Identity and Integrity under the European Convention on Human Rights,* Martinus Nijhoff Publishers, 2009.
- Lock, Tobias, *"The ECJ and the ECtHR: The Future Relationship between the Two European Courts*" The Law and Practice of International Courts and Tribunals. Martinuss Nijhoff Publishers 8 (2009), 375-398.

European Court of Human Rights cases

Association for European Integration and Human Rights and Ekimdzhiev v. Bulgaria,
Handyside v United Kingdom
Huvig v. France,
Klass and others v. Germany,
Kopp v. Switzerland,
Kruslin v. France,
Leander v Sweden,
Malone v. United Kingdom,

Directives and Memorandums

Directive 95/46/EC "On the protection of individuals with regard to the processing of personal data and on the free movement of such data"
Directive 2002/58 "On the processing of personal data and protection of privacy in the electronic communications sector".
European Commission Memorandum no. 14/269, *"Frequently Asked Questions: The Data Retention Directive"*

Decisions of National Courts

Decision no.57, dated 05.12.2014 of the Albanian Constitutional Court
Decision no.33, dated 13.10.2010 of the AlbanianHigh Court
Decision no.129, dated 12.10.2011of the Albanian High Court

Laws

- Law no.7905, dated 21.3.1995 "Criminal Procedural Code of the Republic of Albania Albania"
- Law no. 9918, dated 19.05.2008 "On electronic communications in the Republic of Albania"
- Law no. 9157, dated 04.12.2003 "On Interception of Electronic Communications",
- Law no. 9885, dated 03.03.2008 "On several changes and amendments to law no.9157, dated 04.12.2003 "On Interception of Electronic Communications""
- Law no. 116, dated 12.13.2012 "On several changes and amendments to law

no.9157, dated 04.12.2003 “On Interception of Electronic Communications””
- Law no.8748, dated 01.03.2001 “On Internal Control Service”

Web sites

http://curia.europa.eu/juris/document/document.jsf?docid=150642&doclang=EN
www.legislationonline.org