EUROPEAN ACADEMIC RESEARCH
Vol. VI, Issue 5/ August 2018

Impact Factor: 3.4546 (UIF)
DRJI Value: 5.9 (B+)

ISSN 2286-4822
www.euacademic.org

Protection of Personal Data and Security of Information. The Challenge of Kosovo Institutions that do not Endure the Institutional Vacuum

Dr.Sc. RUZHDI JASHARI
College of Technology and Business - UBT, Pristina
Dr.Sc. MUHAMET AVDYLI
College of Technology and Business – UBT, Pristina

Abstract:

Data protection and information security are two operations and two separate streams that have for target: information security (SI), data protection (DP) in general and personal data protection in particular (PDP). Now, in the MDG and SI efforts, there are many study papers, there are various initiatives. In terms of legal protection of personal data and information security there are; conventions, directives of various international acts. Through the various national regulatory acts, efforts are being made every day to cover and monitor the use of cyber-machine, during processing and transfer of data in the form of information, finalized for use by the users; inside and outside the country. This is due to the fact that: information technology such as processing, the Internet as transferring machinery and the use of social networks as collaborative tools in mobile devices have become a permanent threat to the violation of personal data privacy and information security. Through this paper, we intend to give a modest contribution to this topic, delicate and of interest to us all; as computer users, internet, and social networking in our daily lives.

Key words: Personal data protection, information security, data subject, controller, and misuse of data on the social networks.

Entry

Data protection is a broad term and implies; protection, preservation, security of personal data or data in terms of records or accounts, such as statistical data on the quantity of production, income funds, growth / decrease in production, import or export volume, number of population, the number of pupils or students, the number of patients, the statistics of the diseases, etc., which do not directly correlate with the individual, with personal data and with the sensitive data.

Data, can also be collected, organized or operated through a public or private body, but as such until unfinished for use, they do not play the role of information. However, in practical life, we encounter two types of data that are directly related to the individual; the numerical ones that are further away from the direct link with the individual beyond the individual who referred to relevant data and disorganized data which, while not being processed to be used, and as such these are not information.

In fact, each number, statistical expression, etc. as given, relates to a final point with the individual as a legal or physical person, in the public or private bodies of all social categories of the human society.

During the paperwork elaboration, we provide you with initial knowledge on personal data, personal data subject, information security, knowledge of the differences between data and personal data, open data, information systems, security dimensions protection of personal data and security of information.

Knowledge about data misuse is a duty to know how to protect ourselves from external interference and internal weaknesses.

Personal data

In order to better understand the expression; "Personal data", we first analyze the definitions in the legal framework, what do they say:

The EC 95/46 Directive of the Commission, the Council and the European Parliament of 24 October 1995, Article 2: Personal information means "any information that refers to a natural entity, whose identity is known or can be ascertained" referred to as "the entity" whose identity can be ascertained, is considered the subject that can be determined directly or indirectly, in particular on the basis of the passport number or on the basis of one or more particular data characterizing his physical, biological, psychological, economic, civic or social outlook.

The EU Regulation on the Protection of Personal Data of the Council, the Parliament and the Commission of 24 April 2016/679, has entered into force on 25 May 2018, Article 4:'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable physical person is one who can be identified, directly or indirectly, in particular by referring to an identifier as a name, an identification number, location data, an *online* identifier, or one or more specific identity factors physical, psychological, genetic, mental, economic, cultural or social nature of that natural person".

The definition of personal data, according to the purposes of the *European Convention 108/1981, on the protection of persons with regard to the automatic processing of personal data, adopted by the Council of Europe on 28 January 1981 in Strasbourg, article 2*: it states that: "Personal Data" means any information that relates to an identified or identifiable individual ("subject of data").

By looking at these definitions regarding personal data, according to the legal aspects, we understand that the demotion of personal data is quite extensive. In addition to the personal information of the name and surname, in the everyday life of our various services, we often have to give our sensitive data as well. Sensitive data are sentient and are our privacy. We, our privacy and our data, keep up to ourselves, and it is our will that; we want to share them.

In this set of data fall: biometric data; papillary lines, fingerprints, palm lines, eye retina, profile picture, our picture, genetic data, DNA data, blood group data etc. In addition, the definition of social, political, religious, racial, trade union, scientific, and so on, is also sensitive to the group of sensitive data. The aspects of the intimate life, sex, illness, health, etc. are also sensitive data; personal behavior, conviction and personal choice are individual and belong to the privacy of the individual alone.

Subject of personal data[1]

The subject of personal data is the individual to whom the data belongs and is been related to it. In the theory of personal data protection, legal literature, but also other social markers, we often encounter data on privacy, even as non - property data. In the theory of personal data protection, legal literature, but also other social sciences, we often encounter data on privacy even as non-property data.

The subject of the data is the individual "who, by his will based on the definitions to realize his / her rights in employment, administration, health or other fields of life and work, has declared the non-controlling or employer in accordance with the requirements legal in the respective fields

[1] Dr.sc. Ruzhdi Jashari, PhD Dissertation PROTECTION OF PERSONAL DATA - CASE STUDY REPUBLIC OF KOSOVO, UET, Tirana, 2017

"his personal data. According to the general theory of social law, with the subject of the law we mean any person who enjoys rights and obligations. Only the subject of the right can enter into the kind of relations that are regulated by law and which are called legal relationships (Puto, 2010: 89). The subject data, upon his request, is the legal responsibility of a public or private body, should provide the following information: the regulatory database for data processing, storage, processing purpose, data source, data categories being processed, recipients and categories of data receivers, scope and base (for what purpose they are being processed, for what purpose the entity data was disclosed, including recipients and disclosure of data to other countries).

The data subject has the right to be informed and to know about the technical processing procedures and the involvement in his decision-making. The subject's access to his or her personal data may be permitted at his / her request to copy, transcribe and consult the information at regular intervals, having the right to obtain a copy or extract thereof information. The subject may submit a written request, either electronically or verbally, and the reply from the controller to the data subject should be returned within the legal deadline.

Regarding the possible obstacles and violations noted in this regard by the controller, whether it is public or private, the data subject may address his concern to the state authority for the act, respectively to the AMDhP, in the case of legal violations in The Republic of Kosovo. In case if the subject is dissatisfied, he or she may address it to the ECJ in Strasbourg. The rights and obligations of the Court shall be in conformity with the ratification, signature and acceptance of conventions, respectively directives and regulations, for the signatory states parties of these acts. The subject's expenses for the realization of these rights should be regulated by law, but they are

commonly covered by the controller against whom the complaint was filed.

Whenever the data subject detects irregularities, or if he/she notes from further processing that his interest, image or personality may be damaged, he/she may request from the controller; adding, correction, blocking, destruction, deletion, anonymization and rebuttal of the data. Regarding the undertaken measures, the controller shall notify the data subject in due time, except in cases when it is otherwise defined by law. In case of a breach of these requirements by the controller, the subject / citizen of the data, within an optimal legal deadline, can address the concern to the state authority for the MDP (in this case in Kosovo in the MESP). As long as the application is addressed to the agency, the controller is suspended the further processing of the entity's data processing.

In this case costs for the realization of this right of the data subject are covered by the institution (public or private). However, in addition to persons that have legal capacity, data subjects are also children from birth, persons with disabilities and deceased persons. When using or processing data of these persons, it is mandatory to obtain written consent from their parents, their legal guardians or their authorized persons. The written consent of the subjects of personal data is well regulated in the Regulation 2016/679, (GDPR)

Security of information

The term security of information-InfoSec means the protection of information from unauthorized access, use, disclosure, destruction, modification, reading, inspection or registration. This is a general term that can be used regardless of the form of data that we might get; whether electronic, physical or internet.

But the security of information, especially in present-day IT developments, is only achieved through a disciplined, multidisciplinary approach involving a wide range of activities and rules; local and international, various operational and security systems; different types and classifications of information, including academic upgrading, knowledge, training, organization of human technical and technological resource of work processes with information technology (IT).

Maintaining confidentiality, integrity and information availability (CIA), including aspects of authenticity, accountability, and credibility; are also included as inseparable aspects of information security.

Different scholars have different viewpoints regarding the definition of information security; all points of view merge at a point. For illustration purposes, below we have some definitions regarding information security (IS):

> *"Ensures that only authorized users (confidentiality) have access to accurate and complete information (integrity) when required (availability)." (ISACA, 2008)*
> *"Information security is the process of protecting an intellectual property of an organization." (Vorb, 2000)*
> *".. information security is a risk management discipline, whose job is to manage the cost of information risk to the business." (McDermott and Geer, 2001)*
> *"A well-informed sense of assurance that information risks and controls is in. balance.." (Anderson, J., 2003)*
> *"Information Security is the protection of information and minimizes the risk of exposing information to unauthorized parties." (Venter and Eloff, 2003)*

Information security will be enhanced through our knowledge of the information system, which is an organized combination of: human, hardware (computer hardware), software (program applications), communication networks, data resources,

working methods and data processing. An information system is an organized combination which: supplies, takes, transfers and distributes information within the working organization and, if required or under legal basis it exchanges them with the surrounding, within the country or abroad.

The tasks of the information systems are:

- Data collection,
- Data processing,
- Supply with data and information,
- Distributing data and information to different users by increasing the efficiency and reliability of information security.

The difference between personal data and data

In daily life, with the operation of data in different fields of life and work, globally, with the help of automated computer technology, we process enormous amounts of data. The data can be encountered like:

1. *Numerical statistical quantity - mathematical expression,*
2. *As non-finalized data (date) in process of processing on physical occurrences or business transactions,*
3. *As personal data (PD), in processing or finalized,*
4. *As information, which are source data that have comprehensible content, and are readily available for use by recipients or users of such data in the public and private sector.*
5. *Open data are business, economic, statistical source data that help people in employment and socio-economic development through statistical information on economic, service, commercial, human data etc.*

6. *Data Resources is our knowledge and capacity on business transactions, data processing and organization, Database, etc.*

Who operates with our data? (Personal Data Controller)

According to the Regulation on the Protection of Personal Data of 24 April 2016, No. 679 of the Council, the Parliament and the Commission, article 4 (7) "Controller" , "means a natural or legal person, a public authority, agency or other body, who alone or together with others defines the purposes and means of personal data processing; if the purposes and means of such processing are determined by the law of the Union or of the Member State, the controller or the specific criteria for its designation may be provided by the law of the Union or of the Member State";

Whereas according to Law 03 / L-172 of 29 April 2010 of the Republic of Kosovo "Data Controller" is any natural or legal person from the public or private sector who individually or together with others determines the methods of processing the data, or a person designated by law that also determines the purposes and means of processing ".

Whereas, according to Directive 95/46 / EC of the Parliament, the Council and the Commission of 24 October 1995, Article 2 (d) states that the controller is: "the person responsible of processing, natural or legal person, public authority, server or any other carrier, who together or in collaboration with others, sets the goals and the way of processing personal data. When the aims and methods of processing are determined by the established national or community legal provisions, the person responsible of processing or the specific criteria for its definition may be determined by national law or Community law."

Therefore, controller of the data, in the language of the majority of legislation, since EC and EU law, is the person responsible, principal, chief, mayor or first person in charge of the institution, enterprise, corporation, a public or private body which collects, processes, administers, transfers or retains data in its institution for the performance of the function and duties defined and provided by law, of the body that processes the data of the subjects.

In addition, "the permanent caution of the controller should be at the use of identified or identifiable images and to evaluate privacy issues, including the interests of the parties" (COMMISSION DE LA PROTECTION DE LA VIE PRIVEE, RAPPORT ANNUEL, and Edituer Responsible: M .Debeuckelaere, vzm Atomium-SABAM, Belgium, Brussels, 2010: 38) and data subjects.

The controller's responsibilities towards processing and operation with DHP are regulated by the specific laws of the legal framework of each country individually. The basic regulation on the legal responsibilities of controllers toward the data is provided by the Community Legal Framework of the European Union and the European Council in the he European Convention on Human Rights (Rome, 1950) and its additional Protocols, Convention 108/1981 on automatic processing of personal data, 1995 EC Directive 95/46 on data and privacy, and Regulation 2016/679 of the EC and the EU.

The legal basis of the obligations towards the entities of the data on how the controllers should legally behave during the processing of the data have the laws of the member states of the EC and other non-member states but, in their laws have harmonized Directive 95/46 respectively Regulation 2016/679 of the EC and the EU and have created the authorities for the MDP.

It should be borne in mind that the data subject "during the civil litigation or proceedings in front of a public authority

(e.g. the PRB), to determine whether the data is correct or not may request that at the entry of the file his record should be noted, pointing out that the accuracy is contested and that the official decision is pending."

During this controversial period, the controller of the data cannot, nor should it present the data as finalized and finalized, especially when they are disclosed, given or opened to the receiving parties, and third parties.

According to the rules in force, in accordance with the Directive, respectively the new Regulation on data for all the parties, controllers in order to provide secure data processing are obliged to organize all appropriate organizational, technical measures, including all procedures for the prevention of unauthorized or deliberate unauthorized destruction such as: the reveling, alteration, access or use of data or the sudden or intentional loss of such data, in taking the following actions.

1. protecting premises, equipment and software systems, including access control,
2. protecting application programs that were used for data processing,
3. by preventing unauthorized access to the reading of data in storage and transmission, including their transmission through telecommunications networks and internet networks,
4. by providing efficient methods for blocking, destroying, deleting or anonymizing the data.

Data processed through telecommunications means must be provided in accordance with the measures required by law. Also, hardware equipment, software and application software should be provided in order to provide the appropriate level of security measures for MFSU.

Procedures and measures should be appropriate and up-to-date, taking into account the protection and the risk that

arises during the processing. “According to the principle of accountability, the controller should at all times be able to demonstrate that there is a legal basis for processing his / her data, otherwise processing should be stopped", (Handbook on European Data Preotection Law, European Agency for Fundamental Rights, Council of Europe, Luxemburg Publication Office of the European Union, 2014 : 111).

Officials, employees and controllers who deal with the processing of the data during and after the day's work are obliged to protect the confidentiality of the data they have seen during the processing. Contracted data processors can be entrusted to the processing of data if the contractor is registered in the place where the data supervision is done by an independent national authority mandated by law, where also is the headquarters of the controller, within the limits of authorizations. In that case, the controller shall supervise the implementation of the procedures and legal measures of the contracting authority, including periodic visits of the premises, equipment and spaces where data processing takes place.

Data controllers and processors are obliged in their internal acts to describe in writing the established procedures and measures for the security of the data and to name in writing the people responsible for the file system, who due to the nature of the work should also process sensitive data.

Controllers in public bodies and ultimately private ones are also obliged to name in writing the data protection officer who in some countries in the region and beyond is called a contact point. This is equally binding under the EC legal framework of the Commission and the EU Parliament for protection of the data ("The new regulation of EU, the Parliament and Commission, approved on 24 April 2016")

Insecurity and misuse of internal and social networking data

In various social networking apps, we put, consciously but also negligently, personal information. We are well aware of the many scandals that are related to misuse of our personal information, starting from portals to the most powerful social network in international level. Therefore, even the world's strongest online network "Facebook" has recently been the center of a scandal involving the use of personal data of over 50 million social network users received by Cambridge Analytics. Scandal was revealed for "The Guardian" from a former co-founder of Cambridge Analytics, who in 2016 worked for the election campaign of US President Donald Trump. Companies are accused of collecting data illegally under the guise of a fraudulent app. In the article dated 25 March 2018 "Telegraph" highlights "The EU asks Facebook to pronounce on personal data." Based on this it can be inferred that only on unencrypted devices are safe from data dissemination. Connecting to the Internet, even without giving any data voluntarily, there is a risk of unauthorized access to duplicate data in our computers.
As we speak of the automatic processing of our data in Internet traffic, it is also the era of cybernetics, which is totally different, but it is sealing the new century, our communication and information relations, as well said above, we will address the major groups of insecurity and dangers that come as a result of negligence, our weak knowledge, and the wrong actions.

Providing unnecessary data . It is a risk that leads to the invading of privacy of the individual, but also his / her life. Many applications / forms for free or paid registration for various online services, except for necessary data also contain requests for other data, which are not necessary for completion. Providing unnecessary data is a violation of privacy and may be

detrimental to our personality. The most dangerous actions as non-cautious users are:

1. installing free software without following the installation steps,
2. opening photos, games other than unknown and suspicious addresses,
3. connecting through our personal accounts as; Google or Facebook etc. which gives the right to access and copy different personal profile data,
4. grant access to our accounts; on Facebook, Google or other accounts with the option of downloading any computer or mobile application; we allow you to access and copy personal information with the user's permission

-The risk of using social networks and data bases. In social networks, all of our friends have access to our data depending on the separated privileges. In the case of neglect from one of the "friends" in our list who grants the permission to an application to access his account, it not only collects his information but at the same time it collects also our data for which the "friends" of the list are accessible. The recent case for the intervention of millions of people from whom Facebook is accused of US; see Fareed Zakaria's article brought by telegraph on March 27, 2018; "Discoveries on the use that Cambridge Analytica made of Facebook data - using personal information of more than 70 million users - came at a time when people had already begun to think about finding the right ways to curb that handful of technological companies that dominate not only the US economy, but increasingly American life. "

- Cloud computing. As cloud computing services are global services with good access and low cost for companies, many

companies have gone to cloud computing, avoiding server installation and personal data storage structures. Such a company may be that of a personal physician, a personal architect, a personal researcher, etc. Where the data are recorded and are stored in databases on the Internet.

- **Misuse and uncertainty of data by companies providing services**. This kind of risk is widespread, even among the world-renowned companies such as Facebook where the company does not remove our data even though we have removed our public profiles. Our data remains "permanently" in databases of this company and are used for different company interests. All companies that "live" from customer data through their mechanisms offer suggestions for more efficient use of services; they make incentives for the sale of their products encouraging the purchase of those services that match your wishes. These actions come as a result of the similarity of user interests with the offer compiled on the basis of a pre-planning.

- **The risk of selling our data from companies, either through a secret act or an open act.** In this case, selling through an open act is a lawful sale but may not be compatible with the interests of the user. The risk is presented in cases when smaller companies are purchased from other larger companies where data is bought as part of the package offered without consulting consumers and without the possibility that the consumer initially has the option to remove personal data.

- Third Party Risk. The Internet is an open setting that always has spaces through which everyone can infiltrate; this opportunity is used by different people in order to copy data from different companies. The act of distributing the data to trusted companies poses a risk since they can be attacked by third parties and loses our data. Occasionally, these

occurrences happen when different online services or even those offering different approaches undergo attacks and encounter a loss of privacy of their customers' data. There are different cases like this: Sony's case, the Carbonite data support company, and so on.

- Threats from internal lack of knowledge. From the lack of knowledge of operational staff, irresponsibility and inadequate preparation, etc., abuses happen from:

- Cyber bullying attacks, where interferences in systems come as a result of the human factor.
-potential threats coming from within the system itself, where they are collected and where data is processed, where the security of information is not at the right level.
- From the beliefs, perceptions, lack of knowledge of the individual and the institutions.

- Misuse and exploitation of data for "necessary profiles" or "possible profiles"

This action is carried out by private individuals, from various companies, organizations, as well as from different countries around the world. “Possible Profiles” are those profiles that contain data that can generate information and make it possible for a person to be evaluated as dangerous. This type of confusion usually results from the possibility of different interpretation of the data. “Necessary Profiles” are those profiles that contain data that “meet the conditions” for third parties to achieve the intended purpose either to identity theft or various abuses. http://fjalaime.ch/profili-ne-internet-te-kuptuarit-te-mirat-rreziqet-dhe-keqperdorimi/shikuar në tetor, 2018.

Security and dimensions in data protection.

The field of security sciences is wide-ranging. In the past, security has long been interconnected as "territorial security of states from external interference, as a defense against external aggression or the defense of national interests" or as "global security."

In the period of great technological developments, these concepts are increasingly emerging as inadequate for the time we are living in. Many critics and theoreticians, many new science schools, believe in the creation of "cosmopolitan structures that will better promote freedom, justice and equality around the world in an effort to radically re-evaluate the norms of world politics" (Burchill & Linklater, 2010: 196). Seeing the current global threats such as: international terrorism, major drug cartel developments, problems over environment, wars and ethnic cleansing, health problems, weak states as problematic for world security, poverty, religious extremism, and especially cybercrime; we are called as ever before for unique actions to overcome these challenges.

The good of humanity "internet and telecommunication cybernetics" though it is a great help in our epochal developments for all scientific phenomena to the bringing of new knowledge on the universe, if wrongly used, also causes political, social, financial and explosive nuclear disasters with irreparable consequences for mankind.

Through this approach, to our attention to the necessity for human security, this is best addressed by representatives of the Copenhagen School, especially in the publication "Contemporary Security Studies", an Alan Collins-co-ordinate publication with 23 associates from all continents. Original title "Contemporary security studies"- OXFORD PRES UNIVERSITY, 2013.

"Security is the moment when an issue is presented as an existential threat to a defined referential object" (Collins, 2013: 151).

So when we analyze the violation of information security, abuse of personal information, and abuse of data in general, then in this regard we are dealing with the risk of individual freedoms of the individual and those concerned with protection, processing and data control. The Copenhagen School states that; what we have to deal with is, above all, the concept of "anthropocentric" and obviously the "state-centric" aspect of state stability goes to the fall of individual security called "human security." So the security problem is very tiers and affects all levels of systems organized human life, where personal data is extended. Education should be extended and advanced without delay in:

Social Sciences, Jurisdictional Sciences, Informative Technology Sciences, Security and Privacy Systems Studies, Contemporary Security Studies, Medical Studies, Human Rights and Freedoms Studies, International Relations Studies, in accordance with new developments and inventions of computer technology.

Contemporary security studies, apart from the traditional security sectors, divide studies in " Five Security Sectors: Military Security, Regulatory Security, Economic Security, Social Security, Environmental Security," Collins A. (2013: 20, 21, 22). In this regard, this study required new paths for security studies such as security from terrorism, black trade, computer crimes, transnational crimes, etc. in order for peace to overcome humanity. Seeing the development trend of fast communication, to overcome the challenge of cybercrime is the priority , because each terrorist network, regardless of its activity, is endangering humanity through new cybernetics and telecommunications technology, using its perfect effects, against life and human well-being.

In support of the current legal framework of the Cybercrime Law, MDG Law, Current cyber security strategies, data strategies and program developments in computer science and information technology in our colleges have good predispositions to keep pace with the development trends of this field in the region and beyond. The MDGD in Kosovo from 2016 until today is not functional in implementing the law on mpdh where there is "institutional vacuum". In this situation, there are also and other authorities in Kosovo that burden the development of democracy, respect for human rights, rule of law, and reduce confidence in the decision-making institutions of our country. The concept of security, where we use the computer and our portable devices connected to the Internet and network, can be summarized in: "Individuals, public and private institutions, state, region and beyond;

> *- This concept applies to all sectors of life and work (security, economic, political, information and telecommunications sectors, social networks, health, education, diplomacy, etc.)- This concept of security includes actors; state and non-state. "Theoretical aspect has basic security / mdhp analysis, implemented through rules, institution as a guarantee of security of the dhp with focus on the security of the individual" Jashari.R, UET, Tirana (2017: 55), Doctoral Dissertation MDHP- Case Study Republic of Kosovo.- Human security is set as a priority that requires concrete "security" steps.*

Conclusion

Overcoming this challenge requires academic level knowledge in the field of MFS, in information security systems with particular emphasis on the rule of law and security areas! Therefore it is also required:

1. Drafting of primary and secondary legislation, in line with international legislation, especially with the European one, that is, the alignment with the *aqiqomunitare.*
2. Application of high-standard computerized technology at work and information security.
3. Protection of computers and portal equipment.
4. Operation with data made in accordance with applicable laws.
5. Establishment and appointment of MFA and information security officers in all public and private bodies.
6. Existing vigilance for our personal data; who operates with them? Why and to whom are they transferred? for what purposes? How long do they take care of? etc.
7. Rigorous coverage of rules and legislation, portals and internet service companies and their supervision.

There are many opportunities to influence security enhancement, risk reduction and misuse of data, whatever they may be. In line with this article, we briefly gave some key recommendations on MFS and security of information, knowing that today we have to do with the distribution of billions of information with the data called "Big Data".

Abbreviations

1. AND - Data on research and identification - identity of persons through the DNA in the medical sector.
2. AShMDhP - The State Agency for the Protection of Personal Data
3. AMDHP/AMDhP - Agency for the Protection of Data / Personal
4. BE - European Union

5. DHP - Personal data
6. LMDHP - Law on Protection of Personal Data
7. PD - Personal Data
8. SI - Information Security
9. SHBA - United States of America
10. TI - Information technology
11. MDHP - Protection of Personal DATA
12. Mdhp - protection of personal data
13. dhp - personal data
14. MDH - Protection of data
15. Mdh - protection of data
16. CIA - Confidentiality, Integrity and Aptitude (Availability)
17. UBT -. College of Business and Technology, Pristine
18. UET - The European University of Tirana
19. RKS - Republic of Kosovo
20. KE - European Council
21. GjED - European Court of Justice

Literature used for citations

1. Arben Puto, INTERNATIONAL PUBLIC RIGHT, 2010, revised edition, "Guttenber" Tirana.
2. Alan Collins, CONTEMPORARY SECURITY STUDIES, 2013, OXFORD PRESS UNIVERSITY
3. Dr.sc. Ruzhdi Jashari, Doctoral Dissertation, Personal Data Protection-Case Study Republic of Kosovo, UET, Tirana, 11 May 2017.
4. Handbook on European data preotection law, European Agency for Fundamental Rights, Council of Europe, Luxemburg Publikations Office of the European Union, 2014.

5. Dr.sc.Ruzhdi Jashari, Lecture Cycle of "Privacy and Security of Information Systems", UBT, Pristina, 2018.
6. Work Report of the Belgian Commission for MDHP; COMMISSION DE LA PROTECTION DE LA VIE PRIVEE, RAPPORT ANNUEL, and Edituer Responsible: M.Debeuckelaere, vzm Atomium-SABAM, Belgium, Brussels, 2010.
7. The article; Dennis O'Reilly (March 28, 2011), Privacy: Facebook's Achilles heel, recently visited on May 15, 2014 at the node: http://www.cnet.com/news/privacy-facebooks-achilles-heel
8. European Convention on Human Rights and Freedoms, Rome, 1950.
9. Law on Protection of Personal Data, May 2010, Official Gazette of the Republic of Kosovo
10. Law on Protection against Cybercrime 2012, Official Gazette of the Republic of Kosovo
11. EC 95/46 Directive on the Protection of Personal Data of the Commission of 24 October 1995, of the European Parliament and of the Council
12. Convention on Personal Data Protection in the Automatic Processing of Personal Data and its Additional Protocols 108 of 1981, Strasbourg.
13. Regulation on the Protection of Personal Data 679 of April 24, 2016, which enters into binding force on all EU Member States on 25 May 2018, of the Commission, the Council and the European Parliament.
14. http://fjalaime.ch/profili-ne-internet-te-kuptuarit-te-mirat-rreziqet-dhe-keqperdorimi/, seen in October, 2017
15. Telegraph, 2016, 2017