IMPORTANCE OF THE GEOGRAPHICAL LOCALIZATION OF THE COMMERCIAL PROVIDER OF CLOUD STORAGE SERVICES WITH REGARD TO THE PROTECTION OF CONSUMER'S RIGHTS THROUGH EUROPEAN UNION RULES

IOAN-LUCA VLAD

Doctoral scholarship researcher

"Acad. Andrei Rădulescu" Legal Research Institute of the Romanian Academy

13, Calea 13 Septembrie, corp B, et. 4, sector 5, Bucharest

ROMANIA

ioan.luca.vlad@gmail.com www.icj.ro

Abstract:

The article provides an outline of the issues raised by cloud storage from the perspective of consumer rights in the European Union. Cloud storage, whether of pictures, videos, text messages or other significant personal data involves the distributed storage of such information over a wide network of servers (i.e., "the cloud"), located geographically in several jurisdictions, both within and outside the European Union. While the location of data is dynamic and can even be partitioned (i.e., the information pertaining to one physical person can move from server A to server B and can be also split or shared between them), within the general "cloud", the view of each jurisdiction is static. Thus, each country claims jurisdiction over the information located on servers within that country from the point of view of various legislative enactments. This creates a wide gap between the fundamental assumptions of the legislator and reality.

It is also a fact that the consumer does not and cannot know where the data are located at a particular point in time. When the consumer contracts a cloud storage agreement with a provider, he gives a general agreement regarding the privacy policy of the provider. However, just as usually, the provider does not make specific undertakings, and also contracts cloud storage services from a further, third provider, such as Google, Amazon (who are renowned for their server farms) or others.

The norms of the European Union are established so as to be effective. One of the most problematic areas where personal rights are at stake is that of privacy and the dissemination of personal information. This is because, even though the European Union has very strong legislation on this topic, the fact that data moves outside the Union puts it within the reach of jurisdictions with diluted data protection laws, thus enabling third parties, or government authorities to use the data other than prescribed by the European Union norms.

When such data moves "in the cloud" outside the Union, and maybe even on the servers of a third party "cloud" provider, this provider may, according to its own rules, diminish the level of protection afforded to such data, enabling vast hacking, such as what has happened with Sony Studios after the launch of the movie "The Interview", when millions of data points, including personal identification data and passwords of its users were stolen and exposed on the internet. The risk is such that, by passing into a lesser-protection jurisdiction, information

may be exposed on-line, creating a great image, economic and even personal danger to the consumer.

One method to ensure that such risk is diminished is holding the provider responsible for ensuring the same, high, level of protection for private information as that provided by the European Union. This, in turn, raises a question of jurisdiction over the provider. In other words, whether any particular country in the European Union has jurisdiction to hold the provider to account so as to ensure the respect of the consumer's rights.

The article discusses this issue and posits that the better view is to base jurisdiction on the provider's physical presence because only the consumer protection authorities from such a place have the means and effective contacts required to ensure an efficient communication with the provider, taking proactive steps to protect the consumer's data. The lesser option is for the consumer to appeal to his national courts in order to obtain the protection of his data. However, this option if wrought with obstacles, the most important of which is the dynamic nature of the internet, much unlike the slow-paced approach of the courts. Therefore, for a preventive approach, it is the responsibility of the consumer protection agency of the country where the cloud storage provider is located to ensure a high level of protection for all consumers contracting with that provider, wherever they are located.

***Key-Words**: cloud storage, cloud computing, European Union, data protection, privacy, private international law*

1 Introduction

Cloud storage, whether of pictures, videos, text messages or other significant personal data involves the distributed storage of such information over a wide network of servers (i.e., "the cloud"), located geographically in several jurisdictions, both within and outside the European Union. While the location of data is dynamic and can even be partitioned (i.e., the information pertaining to one physical person can move from server A to server B and can be also split or shared between them), within the general "cloud", the view of each jurisdiction is static. Thus, each country claims jurisdiction over the information located on servers within that country from the point of view of various legislative enactments. This creates a wide gap between the fundamental assumptions of the legislator and reality. Cloud computing places a host of possibilities in the hands of users. However, it also raises significant questions about resources, economics, the environment and the law. One important question relates to geographical considerations related to the data centers that underlie the clouds: physical location, available resources and jurisdiction[1].

Although many users may not be familiar with the term, the reality is that most users of the internet, up to 69 percent, are already taking advantage of cloud computing through Web-based software applications and online data storage services[1]. However, users may not be aware that they are using cloud computing services, because the label is not explicitly attached to the end-interface that they are seeing. Examples of cloud-computing services which involve a large amount of storage are e-mail (Gmail, Hotmail, Yahoo), photo and video services (Flickr, Youtube) and online applications, besides the specifically-targeted file storage and transfer services (Transfer.ro, Wetransfer). Perhaps the epitome of cloud-storage services is the Google Chromebook, which is a new type of laptop, where all the applications (document writer, image processing etc.) are integrated into the browser-based operating system, thus functioning as cloud-based services.

But what is "the cloud"? The cloud appeared as a solution to a practical problem: the exponential growth in the quantity and complexity of information generated by internet activity (from simple text and images creation, to payments systems and complex travel reservation providers), which gave rise to "Web-scale" problems, essentially the issue of supporting millions of transactions a day. In response, technology companies have built increasingly large data centers, which consolidate many servers with associated infrastructure for storage, networking and cooling[1]. The sheer size of these data centers, as well as the expertise of the companies operating them, allowed these providers to offer cloud-storage services to other companies, bringing in an additional source of revenue, while using the down-time of these centers in a meaningful manner.

In essence, Cloud Computing represents a shift from computing as a product that you buy to computing as a service that is provisioned to consumers or enterprises over the network from large-scale data centers, otherwise known as "the cloud"[14]. It is a fact that the consumer does not and cannot know where the data are located at a particular point in time. When the consumer contracts a cloud storage agreement with a provider, he gives a general agreement regarding the privacy policy of the provider. However, just as usually, the provider does not

make specific undertakings, and also contracts cloud storage services from a further, third provider, such as Google, Amazon (who are renowned for their server farms) or others[15].

Where is "the cloud"? It is important to remember that the cloud as a concept is an artificial construct of network administrators, in order to denote the Internet as a resource without having to illustrate its complexity, obfuscating the countless servers, routers, networking cables and other physical infrastructure needed to give it "a life of its own". These servers, contrary to general opinion, are extremely location-sensitive. Among the criteria relevant to choosing the location of a data center are suitable physical space for warehouse-sized buildings, proximity to high-capacity Internet connections, the abundance of affordable electricity but also of cooling agents, the climate and weather, as well as safety of the general area for ease of guarding the location. A very important criterion relates to the laws of the particular country where the data center is located.

What is "personal data"? According to the Data Protection Directive (discussed below), personal data means "any information relating to an identified or identifiable natural person ("data subject"). This includes personal identification numbers, including commercial identification or customer numbers, names, dates of birth, gender, physiology, passwords, account numbers, but also photographs, recordings, and can go on to include bio-metrical data. Departing from this point, "privacy" can be defined as the right to informational self-determination, that is, the right of individuals to know what is known about them, be aware of stored information about them, control how that information is communicated and prevent its abuse[16].

2 The legal framework regarding privacy in the cloud

At the European level, the legal framework regarding privacy in the cloud is given by general European and European Union-specific instruments. From the first category, the two most important instruments are the European Convention for the Protection of Human Rights and Fundamental Freedoms, in particular art. 8 with its expectations of rights of privacy, as well as the more specific Council of Europe Convention 108 for the Protection of Individuals with regard to Automatic Processing of Personal Data.

At the European Union level, the most important instruments are the Charter of Fundamental Rights of the EU, as well as a number of Regulations, Directives, Decisions and other legal instruments regarding the protection of personal data in the electronic communications sector, and the establishment of national agencies tasked with monitoring this protection. They will be outlined in turn.

2.1 International agreements

The most specific international agreement regarding the protection of personal data in the cloud is Convention 108 for the Protection of Individuals with regard to Automatic Processing of Personal Data, adopted under the auspices of the Council of Europe in 1981[2]. In spite of its age, it is still very relevant to the problems of today's cloud computing landscape. The object of the Convention is to strengthen data protection, which means the legal protection of individuals with regard to automatic processing of personal information relating to them.

The reason behind this need is that "information power" brings with it a corresponding social responsibility of the data users in the private and public sector, since many decisions affecting individuals are based on information stored in computerized data files. One major issue identified by the Council of Europe was to what extent national data protection laws afford adequate protection to individuals when data concerning them flow across borders. Although in principle it should make no difference for data users or data subjects whether data processing operations take place in one or in several countries, in practice, protection of persons grows weaker when the geographic area is widened, especially through the use of "data havens" (countries with less strict data protection laws, or none at all)[3].

The Convention has three parts, namely a "common core" of principles which guarantee to all data subjects in all countries where the Convention is in force a certain minimum protection (art. 4-11), a chapter on "transborder data flows" which aims to reconcile the competing requirements of constant availability and fungibility and data protection across borders (art. 12), as well as a part dedicated to mechanisms of cooperation between the Contracting States (art. 13-20). In spite of its relative obscurity, the Convention has been ratified by a large number of states, and has formed the basis for further developments at the European level.

The Convention is supplemented by an Additional Protocol regarding supervisory authorities and transborder data flows, which is much newer, having been opened for signature in 2001[4]. The purpose of the Protocol is to improve the application of the principles contained in the Convention by adding two substantive new provisions, one on the setting up of one or more supervisory authorities by each Contracting State and one on transborder flows of personal data to countries or organizations which are not parties to the Convention. The European Council considered it appropriate for every country to have a data supervisory authority which can provide for an appropriate remedy, as well as sanctions. At the very least, such an authority shall be endowed in national law with powers of investigation and intervention, as well as the power to engage in legal proceedings or bring to the attention of the competent judicial authorities any violations of the relevant provisions. The supervisory authority also serves as an intermediary between the data subject and the controller[5].

In this context it is important to give the definition of the "controller". The "controller" or "controller of the file" is defined in art. 2 of the Convention and means "the natural or legal person, public authority, agency or any other body who is competent according to the national law to decide what should be the purpose of the automated data file, which categories of personal data should be stored and which operations should be applied to them". In more natural words, the "controller" is the person or institution which decides to collect, collects (or causes to be collected) and disposes of the data, either by processing it, or by causing it to be processed, while also disposing of the results of such processing. In practice, to find out who controls the contents and use of personal information kept, the following questions should be asked" who decides what personal information is going to be kept? who decides the use and purpose to which the information will be put? and who decides on the means of processing of personal data? The "data subject" is the person to whom the data pertain, and can well be the end user of a cloud storage service uploading his personal data (such as photos) online.

The Protocol's provision regarding transborder data flows is a compromise between the need for a free flow of information, and the need to provide a sufficient data protection regime. This means that the Protocol opted for the free flow of information inasmuch as the non-signatory state where the data is transferred to has a "satisfactory" data protection regime, and adequacy which is assessed on a case-by-case basis for each transfer or category of transfers made. Since such an assessment is inevitably a very subjective one, Contracting States must provide in their national legislation that controllers of data should provide sufficient safeguards when exporting data to countries whose systems have been judged non-satisfactory from the point of view of data-protection regimes. These safeguards must include contract terms, such as that the data subject has a contact person on the staff of the external partner, whose responsibility it is to ensure compliance with the substantive standards of protection. The data subject should be free to contact this person at any time and at no cost and, where applicable, obtain assistance in exercising his or her rights[5].

In this context, it is important to note what the "processor" means. The processor is the natural or legal person which processes personal data on behalf of the controller. The Controller can be a processor as well, the key difference being that the processor cannot be a controller. There must be a relation of contractual subordination between the controller and the processor, essentially leaving the controller with the responsibility for or control over the personal data. In spite of the very technical and proper principles introduced by the Convention and Protocol, in view of the mechanisms available to the Council of Europe for the enforcement of its Conventions, naturally the impact of these instruments has been limited, generally to the establishment of the basis (groundwork) for further developments at the European Union level.

2.2 European normative documents

The European Union institutions have issued a number of binding normative instruments regarding data protection in the cloud. The most important of these is Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009[6]. This Directive provides for strong rules regarding national data protection authorities, as well as rules concerning the responsibilities of data controllers. Nevertheless, given the technical nature of the field, many other subsequent instruments were needed. The Directive modifies a previous Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002, also known as the Directive on privacy and electronic communications[7]. This Directive addresses principally problems regarding point-to-point communications (telephone, voice over IP etc.), but offers useful principles regarding data protection. The entire legal framework of the European Union on data protection is also applicable to the European Economic Area, under a Decision of the EEA Joint Committee[8].

Another major directive on the protection of personal data is Directive 95/46/EC[9], considered the reference text on the matter. It sets up a regulatory framework which seeks to strike a balance between a high level of protection for the privacy of individuals and the free movement of personal data within the European Union. The main principle of data processing is that it should be lawful, which means that the data subject has unambiguously given his consent, or is a party to a contract for which the processing is necessary, or the controller is

under a legal obligation to process the data, or the processing is in the vital interests of the data subject, or the processing is in the public interest, or of a legitimate interest pursued by the controller or by the third party. In this last situation, the data procession is unlawful if the interests of the controller are overriden by the fundamental rights and freedoms of the data subject.

The data subject has specific rights which are enforceable against the controller, namely, the right to obtain information regarding to the data subject, as well as regarding the controller (identity, purposes of processing, recipients of the data etc.), the right of access to data, as well as the right to object to the processing of data, on legitimate ground. The norms of the European Union are established so as to be effective. One of the most problematic areas where personal rights are at stake is that of privacy and the dissemination of personal information. This is because, even though the European Union has very strong legislation on this topic, the fact that data moves outside the Union puts it within the reach of jurisdictions with diluted data protection laws, thus enabling third parties, or government authorities to use the data other than prescribed by the European Union norms.

In the context of cloud storage services, transfers of personal data from a Member State to a third country with an adequate level of protection are authorized. The determination regarding the adequate level of protection is made by the Member States or by the European Commission, in the latter case its determinations being binding on EU and EEA Member States[11]. Other transfers, such as to a third state which does not offer an adequate level of protection, are authorized within certain exceptions, which are however quite large. Essentially, if the data subject agrees to the transfer then this is permitted. This is, in my view, a very problematic situation. Many of the older users of the internet, such as myself, remember one day when the Yahoo! e-mail service has asked for permission to use its US and other third-countries data centers, this permission being asked at a general level, for all and any of one's e-mail. This option was not offered twice, and, as an user, since opting out, I have always had a slower and more complicated e-mail experience.

Another exception is when there is in place a special type of contract regarding the data that is being transferred between the controller, the data exporter, and a data importer, or a "subsequent sub-processor". This contract was proposed as a model by the European Union [10] and it seeks to ensure that a legal precedence is given to European Union rules, by using choice-of-law clauses. When such data moves "in the cloud" outside the Union, and maybe even on the servers of a third party "cloud" provider, this provider may, according to its own rules, diminish the level of protection afforded to such data, enabling vast hacking, such as what has happened with Sony Studios after the launch of the movie "The Interview", when millions of data points, including personal identification data and passwords of its users were stolen and exposed on the internet. The risk is such that, by passing into a lesser-protection jurisdiction, information may be exposed on-line, creating a great image, economic and even personal danger to the consumer. It is well known that the outcome of a conflict of laws situation is dependent on the state whose courts have jurisdiction over the matter, and it is dubious whether courts of third countries will give precedence to the (stricter) European Union data protection rules.

2.3 Concerns expressed by European consultative bodies concerning privacy in the cloud

Users' expectations of cloud computing involve ease of access, reliability (specifically for mission-critical applications), security of the data, confidentiality and privacy, liability for serious problems, respect of intellectual property, ownership of the data and its use, fungibility (which means that data can be moved between cloud services and within a service with ease, also known as portability), and auditability[1]. These expectations, however, imply a trade-off with the protection of the personal data being processed. Despite the acknowledged benefits of cloud computing in both economic and societal terms, the wide scale deployment of cloud computing services can trigger a number of data protection risks, mainly a lack of control over personal data as well as insufficient information with regard to how, where and by whom the data is being processed[11]. In particular, two potential threats could arise. One is that personal data are processed in different geographic locations within the EEA, which impacts directly on the law applicable to any data protection disputes which may arise between user and provider. The other is that personal data is transferred to third countries outside the EEA, where it may not be safeguarded by appropriate measures.

The European Network and Information Security Agency (ENISA) has identified the following ten security risks that may occur as a result of implementing cloud computing, namely: loss of governance, lock-in (absence of data portability), isolation failure (failure of mechanisms to separate storage, memory and routing between different information controllers renting space in the same server farm), compliance risks (risks to industry certification by moving information into the cloud, particularly in the banking, health and e-payment sector), management interface compromise (i.e., the impossibility of controlling your data stored in the cloud because you temporarily lose access to the interface enabling this control), data protection risks for customers and providers, insecure or incomplete data deletion, and malicious insider risk (i.e., cloud provider employees who have access to the contents of the cloud and use it in a malicious way)[14].

It is important to note that "an international transfer of personal data" does not refer to the posting of information (including personal data) online where it is accessible to anyone who connects to the internet, including people in a third country. The transfer of personal data concerned is only one where the user uploads his data onto a web service, to be processed, with the expectation that such data, while stored in the cloud, will be private. This distinction was made very clear by the Court of Justice[13].

One issue of particular concern was raised in industry circles and involves the integration of services into a "single" cloud-based service. The most commonly given (and seen) example is the travel booking platform, like Expedia, or Orbitz, with an end-interface for the travel agent, and a front-interface for the internet user. This platform might include a customer relationship management application for the travel agent, a travel and accommodation booking and reservations application, a credit card processing application, a financial and accounting application and an e-commerce application, all of which would be seen by the user as a single application[16]. In fact, these applications will usually not be operated by the same cloud provider, nor by the same commercial company. The result is that each element of the

"single" service given to the user has its own privacy policy, its own data protection jurisdiction, its own conflict of laws contractual clauses, which the user usually ignores completely due to time constraints (the pages usually are lost / expired by the time the user has finished reading the relevant legal documents).

Finally, one must also raise the issue of the new 'right to be forgotten', established by the Court of Justice of the European Union. The 'right to be forgotten' is to be welcomed, and it is a natural effect of the Data Protection Directive. However, in the context of the cloud its application is very questionable. To take just one aspect of the problem, if by definition the cloud is dynamic and partitioned, and has a number of back-ups for every particular data point, in order for the 'right to be forgotten' to be effective, one must ensure the deletion of all data points, including the back-ups, which might not be possible particularly if the servers hosting the back-ups are located in a country where there is no such right. Furthermore, the design of the rule's implementation could be such that there is no deletion of the information affecting the data subject, but just a blocking of its release to some geographically-determined users (i.e., the offending search results will not show up to users in Europe, but will continue to show up to users outside Europe). In such a case, the European user can bypass the blocking restrictions by various means (including searching from abroad), making the European Union rules ineffective in this regard.

In order to discuss such issues, a consultative body of the European Union has been set up, entitled the "Article 29 Working Party", which refers to Article 29 of the Data Protection Directive. Its full title is 'the Working Party on the Protection of Individuals with regard to the Processing of Personal Data" and it is one of the bodies competent for interpreting the provisions of the Directive. It carries out this task by issuing recommendations, opinions and working documents on different aspects of the Directive, being composed of representatives of the national data protection authorities of the EU Member States, representatives of the European Data Protection Supervisor and representatives of the European Commission[11].

One proposal put forward by European consultative bodies is that the controller of the data (which the end-user should know the identity of) provides, as a matter of good practice, information relating to the processors and sub-processors providing the cloud services [12]. The problem with this proposal is that such a list, if exhaustive, might be beyond the processing capacities of any human, therefore making it impossible for the end-user to make an informed decision regarding accepting or not the processing of his data. Furthermore, it is completely impractical to request information, much less to begin judicial action, against a large number of data processors.

Another solution found at the European Union – United States level is the "Safe Harbor" framework, which was developed by the US Department of Commerce in consultation with the European Commission. It has been judged as providing an adequate level of protection for personal data. The "Safe Harbor" framework establishes a number of principles and rules which are partly equivalent to the corresponding principles and rules at the European Union level, and involve the existence of contracted persons or companies which assume responsibility for the protection of the user's privacy and protection of data.

Finally, the solution advocated by technology representatives is the use of Privacy Enhancing Technologies / Tools ('PETs'), to establish built-in and proactive privacy best-practices. These would include technologies which strive for data minimization, like encryption, pseudnymisation, anonymisation etc., as well as Transparency Enhancing Tools ('TETs'), providing users with information about privacy policies or granting them online access to their personal data. However, even these circles agree that there is no agreement on what exactly PETs and TETs can mean in practice[16]. One example would be the possibility, now offered by Facebook, of obtaining an 'information report', enabling the user to download everything that Facebook knows about him (personal information, posts, tags, likes, photos, pages, notes etc.). Out of personal experience, reading such a report is overwhelming.

3 Conclusion: the data protection authority as *locus* of the consumer's redress

One method to ensure that privacy risk is diminished is holding the provider responsible for ensuring the same, high, level of protection for private information as that provided by the European Union. This, in turn, raises a question of jurisdiction over the provider. In other words, whether any particular country in the European Union has jurisdiction to hold the provider to account so as to ensure the respect of the consumer's rights.

However, the specialist groups are aware that the complexities of cloud computing cannot be addressed completely via the safeguards and solutions presented above, which provide, however, a sound basis for securing the processing of personal data that EU and EEA-based users submit to cloud providers[12].

The better view is to base jurisdiction on the provider's physical presence because only the consumer protection authorities from such a place have the means and effective contacts required to ensure an efficient communication with the provider, taking proactive steps to protect the consumer's data. The lesser option is for the consumer to appeal to his national courts in order to obtain the protection of his data. However, this option if wrought with obstacles, the most important of which is the dynamic nature of the internet, much unlike the slow-paced approach of the courts. Therefore, for a preventive approach, it is the responsibility of the consumer protection agency of the country where the cloud storage provider is located to ensure a high level of protection for all consumers contracting with that provider, wherever they are located.

References:

[1] Paul T. Jaeger, Jimmy Lin, Justin M. Grimes, Shannon N. Simmons, "Where is the cloud? Geography, economics, environment, and jurisdiction in cloud computing", *first monday*, vol. no. 14, no. 5, 2009, http://pear.accc.uic.edu/ojs/index.php/fm/article/view/2456/2171

[2] Council of Europe, *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data*, opened for signature at Strasbourg, 28 January 1981, http://conventions.coe.int/Treaty/EN/Treaties/Html/108.htm

[3] European Committee on Legal Co-operation, Committee of Experts, *Explanatory Report to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data*, http://conventions.coe.int/Treaty/EN/Reports/Html/108.htm

[4] Council of Europe, *Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data regarding supervisory authorities and transborder data flows*,

opened for signature at Strasbourg, 8 November 2001, http://conventions.coe.int/Treaty/EN/Treaties/Html/181.htm

[5] Council of Europe, *Explanatory Report to the Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data regarding supervisory authorities and transborder data flows*, http://conventions.coe.int/Treaty/en/Reports/Html/181.htm

[6] *Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on coperation between national authorities responsible for the enforcement of consumer protection laws*, Official Journal L no. 337, 18.12.2009, p. 11-36.

[7] *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)*, Official Journal L no. 201, 31.7.2002, p. 37-47.

[8] *Decision of the EEA joint Committee No 83/1999 of 25 June 1999 amending Protocol 37 and Annex XI (Telecommunications services) to the EEA Agreement*, Official Journal L no. 296, 23.11.2000, p. 41-43.

[9] *Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data*, Official Journal L no. 281, 23.11.1995, p. 31-50.

[10] Article 29 Data Protection Working Party, *Working document 01/2014 on Draft Ad hoc contractual clauses "EU data processor to non-EU sub-processor"*, 21 March 2014, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp214_en.pdf

[11] Data Protection Unit of the Directorate-General for Justice, Freedom and Security, *Frequently Asked Questions relating to transfers of personala data from the EU/EEA to third countries*, europa.eu

[12] Article 29 Data Protection Working Party, *Opinion 05/2012 on Cloud Computing*, European Union document 01037/12/EN WP 196, ec.europa.eu/justice/data-protection/index_en.htm.

[13] Court of Justice of the European Union, Case C-101/01, *Bodil Lindqvist*, European Court Reports, 2003, p. I-12971.

[14] Johndavid Kerr, Kwok Teng, "Cloud computing: legal and privacy issues", *Journal of Legal Issues and Cases in Business*, vol. 1, April 2012, p. 1-11.

[15] Lisa J. Sotto, Bridget C. Treacy, Melinda L. McLellan, "Privacy and Data Security Risks in Cloud Computing", *Electronic Commerce & Law Report*, Vol. no. 15, 2010, p. 186-191.

[16] Stephane Guilloteau, Venkatesen Mauree, *Privacy in Cloud Computing*, ITU-T Technology Watch Report, ITU, Geneva, 2012.

Acknowledgement:

This paper is financially supported within the project entitled *"Horizon 2020 - Doctoral and Postdoctoral Studies: Promoting the National Interest through Excellence, Competitiveness and Responsibility in the Field of Romanian Fundamental and Applied Scientific Research"*, contract number POSDRU/159/1.5/S/140106. This project is co-financed by European Social Fund through Sectorial Operational Program for Human Resources Development 2007-2013. Investing in people!