‘Babeș-Bolyai’ University

Faculty of Law

PhD THESIS

PREVENTING ILLEGAL ACCESS TO CLOUD COMPUTING ENVIRONMENT

(table of contents and abstract)

Ph.D. supervisor:
Professor Ioana VASIU, Ph.D.

Ph.D. student:
Bogdan Alexandru URS

Cluj-Napoca

2022

TABLE OF CONTENTS

KEYWORDS

Computing environment; Cloud Computing; cybercrime; illegal access; preventing illegal access; Infrastructure as a Service; Platform as a Service; Software as a Service; Public Cloud; Private Cloud; Hybrid Cloud; Community Cloud; obtaining computer data; security breaches; cyber attacks; cyber fraud; legal prevention mechanisms; technical prevention mechanisms; prevention management mechanisms; prevention in the private sector; prevention in the public sector.

ABSTRACT

The Cloud Computing environment is one of the most important technological developments in recent years, being a true multi-functional phenomenon covering almost all aspects of the digital revolution. From data processing, storage and analysis, to communications, networks and infrastructures, they all come together in one form or another in Cloud Computing services.

In recent years, cyber attacks have become increasingly dangerous and frequent[1]. Their complexity poses a serious threat to the security of citizens around the world. Cybercrime is a major area of criminal law. The sector is vast and technically extremely complex. Moreover, it is constantly changing and diversifying. From a legal point of view, Cloud Computing[2] is a computer environment conducive to criminal activities.

Cloud Computing brings a range of new possibilities for cybercrime. Unlike the early stages of cybercrime, where the focus was on different types of cyber contaminants, in the current period, Cloud Computing creates new possibilities for cybercrime through: computing power, infrastructure, virtual machines, various applications and platforms[3] etc.

[1] UNODC - Expert Group to Conduct a Comprehensive Study on Cybercrime 2021- *Compilation of all preliminary conclusions and recommendations suggested byMember States during the meetings of the Expert Group to Conduct a Comprehensive Study on Cybercrime held in 2018, 2019 and 2020*, p. 19-20, 21, 22. Source https://www.unodc.org/documents/organized-crime/cybercrime/Cybercrime-April-2021/CRP/V2101012.pdf

[2] Wall D. S., *Towards a Conceptualisation of Cloud (Cyber) Crime*, HAS 2017: Human Aspects of Information Security, Privacy and Trust, p. 529. Source https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3038866

[3] Council of Europe - Cybercrime Convention Committee (T-CY), *Criminal justice access to data in the cloud: challenges*, Discussion paper prepared by the T-CY Cloud Evidence Group, T-CY (2015)10 Provisional, 26 May 2015 Strasbourg, France, p. 9-11. Source https://rm.coe.int/1680304b59

Illegal access in the Cloud Computing environment is a key element for understanding the whole criminal phenomenon, as it creates opportunities for other, more serious and dangerous cybercrimes. Essentially, the crime enables the execution of extremely dangerous cyber-attacks, which can take the form of other cyber-crimes such as: computer fraud, fraudulent financial transactions, illegal interception of a computer data transmission, alteration of the integrity of computer data, disruption of the functioning of computer systems, unauthorised transfer of computer data, computer forgery, extortion, computer sabotage, copyright offences, terrorist offences, etc.

Illegal access to the Cloud Computing environment and associated cybercrime is a global phenomenon and therefore a global response is needed to tackle it. Preventing illegal access to Cloud Computing is one of the most effective strategies to combat the phenomenon, which is spreading at the same pace as the development and spread of information and communication technology[1].

The first title of the thesis (Cloud Computing - the computing environment) was structured in two chapters. The first chapter covers preliminary aspects and the second is dedicated to the computing environment and Cloud Computing technology.

We started **the first chapter** with some preliminary aspects related to the research objectives and methodology. Next, we briefly outlined the motivation for choosing the topic and the current status of the research.

A first research objective was to study the Cloud Computing environment and its peculiarities. We defined the computing environment and explained each feature of Cloud Computing technology (own on-demand services, access to services via a network or the Internet, dynamic resource allocation, flexibility of services, etc.).

The second objective of this paper is access to the Cloud Computing environment. We have chosen to present at a conceptual level, without going into excessive technical detail, the mechanisms for controlling access in the Cloud Computing environment. After researching how legal access is done in Cloud Computing, it was necessary to study how illegal access is done in Cloud Computing.

The third objective of this paper and the most important part of our research is the prevention of illegal access in the Cloud Computing environment. The research objectives

[1] Brewer R., Vel-Palumbo M., Hutchings A., Holt T., Goldsmith A., Maimon D., *Cybercrime Prevention Theory and Applications, Crime Preventionand Security Management*, ISBN 978-3-030-31068-4 ISBN 978-3-030-31069-1 (eBook), https://doi.org/10.1007/978-3-030-31069, p. 2, 3-5. Source https://link.springer.com/book/10.1007%2F978-3-030-31069-1

outlined above focus on this last and extremely important objective. The analysis of current issues related to the prevention of illegal access lies at the core of our work. Preventing crime means finding the most effective practical solutions. Whether legal, technical or managerial prevention methods, they are all indispensable for the security of the Cloud Computing environment. The study of these methods and their implementation is an appropriate research objective for our chosen interdisciplinary field. Given the multidisciplinary approach of the research, throughout the paper we have chosen to consult the scientific literature in both the legal and information and communication technology fields.

Illegal access in the Cloud Computing environment is a complex crime from both a legal and technical point of view. Preventing such a crime requires a new approach as illegal access has a direct impact on other cybercrimes. We have chosen this research topic even though its study is quite difficult as it requires both legal knowledge and advanced practical knowledge in the technical field of the information and communication industry.

In chapter two, we set out to examine *in extenso* the notion of 'computing environment' and Cloud Computing technology. Essentially, the *'computing environment'* is a set of hardware and software elements operating as a unit within information systems and networks, performing different functions and interactions (between information systems or between people and information systems)[1]. *Cloud Computing* is a model that enables easy and ubiquitous access via a network to a set of configurable computing resources (networks, servers, storage, applications, services and more), which can be launched and delivered with minimal management tools and little interaction from the service provider[2]. Cloud Computing technology has the following characteristics: dynamic allocation of computing resources, access to the Cloud is provided over a network (Internet), services are provided on demand and are flexible and quantifiable. The three common *delivery* models for Cloud Computing services are: 'Infrastructure as a Service' (Iaas), 'Platform as a Service' (PaaS) and 'Software as a Service' (SaaS). Generically there are four models for *implementing* Cloud Computing services: Public Cloud, Private Cloud, Hybrid Cloud and Community Cloud.

The second title of the thesis (Cloud Computing Access and Cybercrime)is a broad analysis of how legal access is done in the Cloud Computing environment. Starting from this, we then moved on to the study of the offence provided for in Article 360 of the Criminal

[1] This definition was published by Urs B., *'Cloud Computing – mediul propice pentru criminalitatea informatică',*'Dreptul' Magazine nr. 3/2018, , p. 142-143, ISSN 1018-0435, UJR Bucharest 2018.

[2] The National Institute of Standards and Technology (NIST), *The NIST Definition of Cloud Computing*, Recommendations of the National Institute of Standards and Technology. Source http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf

Code, with express reference to illegal access in the Cloud Computing environment. Next, I explained in detail the implications of illegal access on the dynamics of the criminal phenomenon existing in the Cloud Computing environment.

The first chapter in this title is dedicated to legal access in the Cloud Computing environment. It involves following pre-established steps and procedures. Beyond the technical aspects, it is essentially about those mechanisms and models that play a role in authenticating and authorising users who legally access Cloud Computing services. User access takes place in a controlled environment, where each user has various functions and restrictions, which are designed to maintain security in Cloud Computing. Within the control systems, authentication and authorisation mechanisms are automatically configured according to the requirements of the service providers.

In the second chapter we noted that although a number of control systems and mechanisms are in place, illegal access in the Cloud Computing environment is still a serious problem for the security of the computing environment. The offence of illegal access to a computer system is regulated in Article 360 of the Romanian Criminal Code. After examining the legislation criminalising the offence in the United States of America, the United Kingdom of Great Britain and Northern Ireland, Australia, Germany and France, we found that there is no consensus on the criminal conduct.

The crime of illegal access to the Cloud Computing environment is a dangerous crime. Illegal access to a computer system is a predicate offence, or in other words a ‘platform’ that makes other computer crimes possible[1]. In most cases we can talk about illegal access being a means to an end crime The offence mainly enables dangerous computer attacks that can take the form of other computer crimes, such as: computer fraud, fraudulent financial transactions, illegal interception of a computer data transmission, alteration of the integrity of computer data, disruption of the functioning of computer systems, unauthorised transfer of computer data, computer forgery, blackmail, computer sabotage, copyright offences, terrorist offences and others.

In the meaning given by the Romanian legislator, Cloud Computing is such a computer system, in the sense that it contains both *hardware*, and *software* components whose function is the automatic processing of computer data by means of computer programs. Illegal access to Cloud Computing essentially involves penetrating (either directly or remotely) the components that make up the computing environment. *‘Access’* means the

[1] Vasiu I., Vasiu L.,*Criminalitatea în cyberspațiu*, Universul Juridic Publishing House, Bucharest 2011, p. 144

ability to logically interact with all or part of the computer system/Cloud Computing environment, allowing the possibility to access computer resources, to modify system functions or to launch various commands in the system, either directly locally or remotely via a computer network.

In our view, whether it is a matter of a committing or an omissive attitude (maintaining access), breaking into the computer system constitutes the essential element of the offence. The criminal legislator has introduced an essential condition, namely that the criminal activity must be carried out ‘without right’. In essence, lack of authorisation is a constituent element of the offence, although substantive criminal law refers to illegal or ‘unlawful’ access. In practice, from the point of view of the offence of illegal access to a computer system, the Romanian legislator has considered a wider range of options which include both the notion of ‘illegal’ and that of ‘unauthorised’ or ‘without right’, which are rather interchangeable notions[1].

The first aggravated form of the offence of illegal access to the Cloud Computing environment is provided for in Art. 360 para. (2) of the Criminal Code and is aimed at obtaining computer data. As explained above, the Cloud Computing environment consists of a set of essential elements, computer data being one of them. It is not necessary in this case that the purpose is to achieve and obtain computer data. Moreover, if the particular purpose existed previously and access is in the basic form, it is sufficient for the aggravated form of the offence. The second aggravated form of the offence of illegal access to the Cloud Computing environment is provided for in Article 360 (2) of the Criminal Code. (3) of the Criminal Code and involves violation of security measures.

The Cloud Computing environment, architecture and services are protected by means of specialised procedures, devices and software, and access is generally restricted or prohibited for certain categories of users. Security measures mean specialised procedures, devices or software, whereby access is restricted or denied to certain categories of users. Even though a number of security measures are listed in the text of the law, it is sufficient for the aggravated offence to be committed if only one measure is breached. It is not enough for the security measures to exist, they must be in place, and a circumvention of their functionality is necessary to retain this modality.

[1] Zlati G., *Tratat de criminalitate informatică*, Vol. I, Solomon Publishing House, Bucharest, 2020, p. 216

The characteristics of the Cloud Computing environment have a direct impact on the ways in which the offence of illegal access to the computer environment is committed. Cloud Computing is not just a computer system. Thus, a first step and a particular feature of committing this crime is to determine exactly what is to be illegally accessed. The second particularity or stage prior to the actual access to the Cloud environment is the recognition or collection of as much information as possible about the environment or service to be illegally accessed. The steps necessary to establish the mode of action and reconnaissance are merely preparatory acts for the commission of the offence of illegal access to the Cloud environment. Another feature of the essence of the offence of illegal access to the Cloud Computing environment is the default mode of action.

Illegal access in the Cloud Computing environment can be carried out either at the level of architecture and infrastructure (servers, storage and network equipment, VMs, etc.) or at the level of applications and services (productivity tools, 'VoIP' communication, email, 'backup', etc.). Strictly from a technical point of view, access at the infrastructure level is much more difficult to achieve than access at the application level as it requires advanced knowledge of vulnerabilities as well as complex methods to exploit them. Finally, maintaining access and hiding the traces of crime are operations adjacent to the crime of illegal access in the Cloud Computing environment.

Illegal access in the Cloud Computing environment remains problematic from a jurisdictional point of view. Criminal law enforcement and the process of dispensing justice are key issues of a state's sovereignty. Jurisdiction in criminal matters is closely linked to the geographical territory of that state. In analysing and studying cases of cybercrime, we have noted that illegal access to the Cloud Computing environment has involved acting remotely, sometimes even from other countries. The international element of illegal access to the Cloud environment and other related cybercrime is frequently encountered in such situations. Therefore, a number of jurisdictional issues arise, but also some conflicts of jurisdiction. It is very important to note that international cooperation does not affect the sovereignty of states, their jurisdiction or their national law.

Jurisdictional and territorial issues in the Cloud Computing environment derive from the foreignness components relevant to the dynamics of crime. The operation of a varied spectrum of relevant jurisdictions in different countries can lead to a situation where several countries claim jurisdiction over a cyber crime of illegal access. Conflicts are often of a competitive nature. They are caused by various shortcomings that exist at the level of legislative regulation. In general, in such cases it is necessary to have specific legislation at national level on the resolution of conflicts of jurisdiction. Moreover, it would be advisable for the states concerned to find solutions through consultation and, why not, even to work together to find the optimum jurisdiction[1]. We are of the opinion that when a cyber crime of illegal access to Cloud Computing or a crime with cloud implications has been committed, it is possible that the crime falls under the jurisdiction of several states.

In the third chapter we looked at how illegal access affects the Cloud Computing environment. Cyber-attacks play a crucial role in committing the crime of illegal access in the Cloud Computing environment. Studying the specifics of these cyber attacks has allowed us to identify the complex mechanisms that generate illegal access and the criminal phenomenon associated with it. It is important to note that the characteristics of cyber attacks closely follow the characteristics of the Cloud Computing environment. Each attack has a number of characteristics and peculiarities, which once materialised, give rise to complex forms of cybercrime. In our research we have analysed in detail authentication and authorisation attacks, wrapper attacks, sidechannel attacks, Man in the Cloud attacks, Man in the Middle attacks and insider attacks. From a legal point of view, Cloud Computing is a computer environment conducive to criminal activities.

In our view, the big problem with this complex computing environment is the migration from traditional digital crime to the complex digital crime that is present in Cloud Computing. In other words, it is the migration from a cybercrime based on somewhat limited computational resources (e.g. a proprietary computer system) to a digital crime with virtually unlimited resources (in terms of infrastructure, platform and applications). The migration of users to Cloud Computing automatically leads to the migration of cybercrime. There are currently two main categories of crime in Cloud Computing: in the first category, *the computing environment is the target of the crime*, and in the second category, the Cloud environment is used as a *tool to commit the crime*.

The third title of the thesis (Preventing illegal access in the Cloud Computing) contains a rigorous analysis of how cybercrime prevention mechanisms are organised and operate. Our research focuses on the study of legal, technical and managerial mechanisms for

[1] See Urs B., '*Investigațiile digitale în mediul Cloud Computing. Probleme și soluții*', Section published in 'Dreptul' Magazine No. 7/2019, p. 187-188, ISSN 1018-0435, UJR Bucharest 2019.

preventing cybercrime. With regard to the prevention of illegal access in the Cloud Computing environment, we opted for a differentiated approach depending on the role of the public and private sector. The research study carried out on the main companies providing Cloud Computing services in the country and abroad was of great help in this scientific approach.

We started the **first chapter** of the third title with the methodological organisation of the existing cybercrime prevention mechanisms in the Cloud Computing environment. Essentially, these are implemented at a principle level. Prevention of cybercrime is one of the most effective mechanisms to combat the phenomenon. Prevention focuses on regulating and mitigating risks, and in the context of cybercrime, the mechanism aims either to prevent the occurrence and recurrence of illegal activity, or at least to mitigate the harm resulting from its commission. Preventing cybercrime in the Cloud Computing environment is a complex process from a legal, technical and managerial point of view. Addressing such a phenomenon solely from a technical point of view is not sufficient, even if at first glance the technical side is of particular importance in terms of the environment and the architecture of the Cloud Computing infrastructure. Without legal and managerial elements, technical prevention methods lose their effectiveness. This is the proportionality ratio between the number of incidents or cybercrimes and the number of incidents that were prevented or did not have an effect.

Approaching prevention from the perspective of users, the private sector and the state is likely to encompass a broad spectrum of mechanisms and measures, regardless of the parties involved. From our research we have identified that the pattern and degree of use of Cloud Computing services is correlated with the user experience - a concept that derives from the interaction between users and the services used[1]. The user experience directly reflects on the quality of Cloud Computing services and implicitly on the dynamics of the criminal phenomenon occurring in the Cloud Computing environment. The effectiveness of forms of

[1] Urs B., Rusu C., Rusu V., Botella F., Quinones D., Urs I.,. Morales J., Cano S., Aciar S., Castro I. B., *'Forming Customer eXperience Professionals: A Comparative Study on Students' Perception'*, paper published in Systems Engineering and Design II, Proceedings of the 2nd International Conference on Human Systems Engineering and Design (IHSED2019): Future Trends andApplications, September 16-18, 2019, Universitat der Bundeswehr Munchen, Munich, Germany, Edited Springer Book (2nd ed. 2019, XXI, 1105 p., ISBN 978-3-030-27928-8, DOI 10.1007/978-3-030-27928-8, T. Ahram et al. (Eds.): IHSED 2019, AISC 1026, pp. 391–396, 2020, https://doi.org/10.1007/978-3-030-27928-8_60, p. 392. Source https://link.springer.com/chapter/10.1007%2F978-3-030-27928-8_60.

cybercrime prevention varies greatly depending on which Cloud Computing services are chosen based on user experience[1].

Chapter two focuses on those legal measures with a preventive role. Applicable criminal law sanctions are a highly effective mechanism in preventing illegal access and other related cybercrime. On the prevention side, the deterrent function of the criminal law leads the person intending to commit a cybercrime to weigh the risks of his conduct against the sanction involved[2]. In addition to criminal law rules, there are other pieces of legislation with direct implications for preventing illegal access to the Cloud Computing environment. One such act is EU Directive 2016/1148 on measures for a high common level of network and information systems security. The Directive is part of the European Commission's cyber security strategy for the European Union and was created to enhance cooperation between EU Member States on cyber security issues by imposing minimum harmonisation rules. Cloud Computing is one of the drivers for the reform of data protection legislation. The Data Protection Regulation (EU) 2016/679 is directly applicable in all EU Member States and updates data protection legislation so that on the one hand the rights of individuals are protected and on the other hand it allows companies to use personal data in a transparent manner across the EU. Cyber-attacks targeting the Cloud Computing environment are covered by Directive 2013/40/EU, which lays down minimum rules on the definition of criminal offences and sanctions. In addition, it improves cooperation between authorities, but also between specialised bodies such as Eurojust, Europol, the European Cybercrime Centre and the European Network and Information Security Agency (ENISA).

Chapter three deals with technical security mechanisms to prevent illegal access. Technology security is an essential component in the process of preventing illegal access in the Cloud Computing environment. Security measures comprise a series of standards, legal provisions, user policies and procedures, security principles but also contractual obligations acting at the physical, operational, managerial and procedural levels. Their implementation actively contributes to the fight against cybercrime and the mitigation of its negative effects. The security of the Cloud Computing environment can be seen in terms of the two parties involved: the user and the service provider. The responsibility for the security of the

[1] Tabrizchi H., Rafsanjani M. K., *A survey on security challenges in cloud computing: issues, threats, and solutions*, The Journal of Supercomputing volume 76, pages 9493–9532 (2020), Springer, https://doi.org/10.1007/s11227-020-03213-1, p. 6, 15. Source https://ibook.pub/a-survey-on-security-challenges-in-cloud-computing-issues-threats-and-solutions.html

[2] Streteanu F., Nițu D., *Drept penal. Partea generală*, Vol. 2, Universul Juridic Publishing House, Bucharest, 2018, p. 278-279, 282.

computing environment is thus divided: the provider is responsible for the security aspects of the environment and infrastructure, and the user is responsible for the security of the operation of the system, the applications and the data used.

From a technical point of view, preventing hacking and protecting data in Cloud Computing requires the use of various technologies. These include the use of a secure connection (SSL/TLS), the creation of a Virtual Private Cloud (VPC), access via a Virtual Private Network (VPN), data encryption with the AdvancedEncryption Standard (AES) algorithm, etc. Encryption is currently one of the most effective methods of protection against illegal access. Encrypting data helps both to increase the level of security in the Cloud Computing environment and to make it more difficult to gain illegal access. The most important encryption methods analysed include hash encryption, traditional ('symmetric') encryption, two-key ('asymmetric') encryption and homomorphic encryption.

Chapter four deals with the management side of mechanisms to prevent illegal access in Cloud Computing. The organisational principles of Cloud Computing services are fundamental elements of data and infrastructure protection and provide users and providers of Cloud Computing services with a starting point for assessing the computing environment and its security. The organisation of a security framework in a Cloud Computing environment is done by the service provider. The process consists of implementing security controls and recommending remedies to security problems in the system (configuration management, vulnerability analysis, preventive monitoring and incident management). Service security management and auditing tools play a key role in preventing illegal access in the Cloud Computing environment. Structured management and auditing are likely to contribute directly to a significant reduction in illegal access offences and even deter any such attempts.

Today there are a number of expert organisations such as the Cloud Security Alliance (CSA), the International Organization for Standards (ISO), the National Institute for Standards and Technology (NIST), the European Union Agency for Network and Information Security (ENISA) and others. These organisations are working to implement security standards in the Cloud Computing environment and to find solutions to user and service provider security issues. These standards include ISO/IEC 27017:2015, ISO/IEC 27018:2014, ISO/IEC 27036:2016, PCI-DSS, HIPAA/HITECH, FedRAMP, FIPS 140-2 etc.

Chapter five deals extensively with the role of the public sector in preventing illegal access in the Cloud Computing environment. Preventing cybercrime through criminal prosecution is a highly effective measure, as penalties are designed to deter offenders. Prosecution and the process of justice require proving cybercrime beyond any doubt, which requires electronic evidence. National policies and strategies to prevent cybercrime play a key role in the Cloud Computing environment. In Romania there is a general government policy on the protection of personal data and international cooperation contributes significantly to prevention through criminal investigation procedures. We also stress the importance of digital investigations in preventing and combating illegal access in the Cloud Computing environment. Detecting and holding accountable cyber criminals is an important part of prevention.

The complex nature of the Cloud Computing environment creates problems in investigating cybercrime. Legislative differences in multiple jurisdictions further complicate these criminal investigations. Investigating crime in a decentralised IT environment requires the ability to collect computer data in the form of digital evidence that crosses national borders. Unlike traditional methods of investigating computers and various singular devices (which have a centralised nature of computer system operation), in investigations conducted in Cloud Computing there is no complete control over forensic artefacts (routes, logs, storage items etc). Three types of data are essential for any Cloud Computing investigation: user or subscriber information, traffic and connection data over the Internet or other network, and content data stored in the Cloud[1]. The whole course of an investigation depends on obtaining this data.

Chapter six explored the role of the private sector in preventing illegal access in the Cloud Computing environment. The procedures involved in securing and preventing illegal access and other cybercrime in the Cloud Computing environment are rules that must be followed and implemented by service providers and users. They are designed to ensure the security of the Cloud Computing environment, systems and infrastructure at physical, operational and procedural levels. While security policies refer to the prevention of various intentional or unintentional security incidents, cybercrime prevention policies refer to those incidents which, according to legal provisions, are considered as crimes. The risk posed by illegal access to the Cloud Computing environment and other related cybercrime is estimated

[1] Council of Europe - Cybercrime Convention Committee (T-CY) - *Criminal justice access to electronic evidence in the cloud: Recommendations for consideration by the T-CY Final report of the T-CY Cloud Evidence Group*, www.coe.int/cybercrime, 16 September 2016 Strasbourg, FranceT-CY (2016)5, p. 12. Source https://rm.coe.int/16806a495e

based on the probability of an incident. In Cloud Computing, probability is associated with the negative impact of the incident on the computing environment. The direct action of service providers on the Cloud Computing environment is reflected in the detection, prevention and mitigation measures they implement or do not implement, precisely to reduce or even eliminate the risk posed by a particular vulnerability or cybercrime.

Service providers are the main impact factor with regard to the security of the IT environment, data protection, the evolution of the drivers of crime and their role in preventing illegal access in the Cloud Computing environment. The study of the main Cloud Service Providers in the country and abroad aims to explain how they implement security policies and prevent illegal access and other cybercrime in the Cloud Computing environment. Our research focused on analysing existing security techniques at the level of Cloud Computing service providers (Google Cloud Platform, Amazon Web Services, Microsoft Azure, IBM Cloud Computing and Sistec IT Solutions.) and assessing how these companies act to protect personal data.

In conclusion, we believe that preventing illegal access in the Cloud Computing environment is an appropriate research problem for this interdisciplinary field. From our research, we found that preventing illegal access is one of the most effective ways to combat crime in the Cloud Computing environment. We have explained that prevention is essentially a new and complex phenomenon from a legal, technical and managerial point of view. In the course of our research, we have identified a number of tools and mechanisms that directly contribute to the prevention of illegal access in the Cloud Computing environment. First of all, it should be noted that preventing illegal access in the Cloud Computing environment requires changes in the legislative field. These changes include the imposition of measures on Cloud Computing service providers aimed at strengthening security requirements, simplifying incident reporting obligations, introducing more effective surveillance measures and much stricter enforcement requirements, including new penalty regimes. Secondly, it is necessary to highlight the role of the service provider. Although there are differences in the technical prevention solutions that these companies implement, we believe that every measure counts, whether it is IDS and IDPS, Virtual Private Cloud, virtual machine isolation and the like. Thirdly, we are convinced that, in order to prevent and combat the criminal phenomenon, which has taken on global proportions in recent years, a common basis for action is needed and, of course, investment in extensive research into it, both at academic level and at the level of decision-makers. Finally, we can only hope that our research efforts will have a direct impact on the criminal law literature.