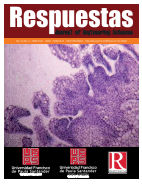
Respuestas, 24 (3), September - December 2019, pp. 15-25, ISSN 0122-820X - E ISSN: 2422-5053



Respuestas
Journal of Engineering Sciences
RESPUESTAS

Original Article

https://doi.org/10.22463/0122820X.1845

Impact on personal security against the regulation of cybercrime at the University of Pamplona, Villa del Rosario headquarters

Impacto sobre la seguridad personal frente a la regulación de la ciberdelincuencia en la Universidad de Pamplona, sede de Villa del Rosario.

Tatiana Valentina Ovalle-Lizcano[1]*, Diego Luis Coronel-Peñuela[2], Rocío de Belén Contreras-Manrique[3], Alfonso Cabrera-Reyes[4], Liliana Contreras Manrique[5]

1 Abogada en formación, tatiana.ovalle@unipamplona.edu.co, ORCID: 0000-0003-3643-8584, Universidad de Pamplona, Pamplona, Colombia.*
2 Abogado, dlcp11@hotmail.com, ORCID: 0000-0003-0580-1109, Universidad de Pamplona, Pamplona, Colombia.
3 Magíster en Prácticas Pedagógicas, rociodebelen@unipamplona.edu.co, ORCID: 0000-0002-4434-0408, Universidad de Pamplona, Pamplona, Colombia.
4 Abogado, alphonsocabrerar@hotmail.com, ORCID: 0000-0002-1611-7284, Universidad de Pamplona, Pamplona, Colombia.
5 Magister en Orientación. lilianacontrerasmanrique@yahoo.com.mx, ORCID: 0000-0002-8586-2093, Universidad Francisco de Paula Santander, Cúcuta, Colombia.

How to cite: T. Ovalle-Lizcano, D. Coronel-Peñuela, R. Contreras-Manrique and A. Cabrera-Reyes, L. Contreras-Manrique, "Impact on personal security against the regulation of cybercrime at the University of Pamplona, Villa del Rosario headquarters". *Respuestas*, vol. 24, no. 3, pp. 15-25, 2019.

Received on January 30, 2018 - Approved on June 10, 2018

Keywords:

Colombian criminal code,
Constitution,
Computer crimes,
Virtual theft,
Social networks Security against the regulation of computer crimes.

ABSTRACT

Computer crime and its evolution in Colombia, is relevant, the computer crimes described in Law 1273 of January 5, 2009 on the protection of information and data. Therefore, in the political constitution, article 15. All persons have the right to their personal and family privacy and their good name, and the State must respect them and enforce them, also, they have the right to know, update and rectify the information that they have been collected on them in databases and in archives of public and private entities. For this reason, cybercriminals, have specialized mainly in theft through computer means, this being the most common cybercrime in the city of Cúcuta, where citizens have been affected by this criminal modality in recent years. The research has a quantitative, non-experimental approach and the research design is descriptive-purposeful, random sampling and a sample of 100 students from the University of Pamplona, a questionnaire was applied. Results and analysis. The first category in social networks stood out, 84% in students responded that Yes, They have seen how the privacy of another person is exposed by the incorrect handling of information, photos, videos, etc., in social networks; Next, 95% of the students responded that Yes, they would like more information about computer crimes and information about their prevention and virtual theft category, 53% of the students answered that Yes, they know people victims of virtual thefts. To finalize, it is relevant that they provide information and guidance through training meetings and in turn implement group strategies to raise awareness in the educational community through personal security against the regulation of computer crimes.

Palabras clave:

Código penal colombiano,
Constitución,
Delitos informáticos,
Hurto virtual,
Redes sociales,
Seguridad frente a la regulación de los delitos informáticos.

RESUMEN

La delincuencia informática y su evolución en Colombia, es relevante, los delitos informáticos descritos en la ley 1273 de 5 de enero de 2009 de la protección de la información y los datos. Por lo tanto, En la constitución política, artículo 15. Todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar, también, tienen derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos y en archivos de entidades públicas y privadas. Por tal motivo, los delincuentes informáticos, se han especializado principalmente en el hurto a través de medios informáticos, siendo este el delito informático de mayor ocurrencia en la ciudad de Cúcuta, donde los ciudadanos, se han visto afectados por esta modalidad delictiva en los últimos años. La investigación tiene como enfoque cuantitativo, no experimental y el diseño de la investigación es descriptivo- propositivo, un

***Corresponding author.**
E-mail address: tatiana.ovalle@unipamplona.edu.co (Tatiana Valentina Ovalle-Lizcano)

muestreo al azar y una muestra de 100 estudiantes de la Universidad de Pamplona, se aplicó un cuestionario. Resultados y análisis. La primera categoría en las redes sociales se destacó, un 84% en los estudiantes respondieron que Si, Han visto como la intimidad de otra persona queda al descubierto por el incorrecto manejo de información, fotos, vídeos, etc, en las redes sociales; seguidamente, un 95% en los estudiantes respondieron que Si, quisieran tener más información sobre los delitos informáticos e información sobre su prevención y la categoría hurto virtual, un 53% en los estudiantes respondieron que Si, conocen personas víctimas de hurtos virtuales. Para finiquitar, es relevante que suministren información y orientación a través de encuentros formativos y a su vez implementar las estrategias grupales para concientizar a la comunidad educativa a través de la seguridad personal frente a la regulación de los delitos informáticos.

Introduction

The new information and communication technologies from the twentieth century to the present, has been a tool of great benefits, since it is possible to interculturalize and exchange information achieving socio-economic activities worldwide, thus being closer interaction with other people, however, also have their disadvantages or dangers that generate organizations in computer crime, arising the computer crime or theft crimes, contemplated in Law 1273 of 2009 (Article 2691). Therefore, the criminal treatment is that of qualified theft, enshrined in Article 240 of Law 599 of 2000, which is obtained to a prison sentence of six (6) to fourteen (14) years, according to the circumstances of time, mode and place [1].

Ojeda et al. [2], described and analyzed the evolution and conceptual framework of the computer crimes proposed by different national and international authors, and establishes the relationship with the recent Law 1273 of 2009, by means of which the Colombian legislation will be equated with that of other countries as for the normativity on cybercrime, which has been violating different fields of relations and personal, business and institutional communications. Cybercrime, as a trend that affects not only the technological field but also the economic, political and social, must be known, evaluated and confronted, so the analysis of the rule, its contribution and scope can give other elements of judgment to understand the reality of our organizations and visualize their policies and strategies, in light of the same rule and global standards on computer security [2].

Due to the above, research was carried out on the analysis of the regulation of computer crimes through the impact on the fundamental rights of individuals so that their individual, collective security is not violated at the University of Pamplona headquarters Villa del Rosario; By which the Colombian normative framework for the regulation of computer crimes through the penal code is recognized, in a second order the computer crimes were categorized through the incidence in the fundamental rights of people so that their collective individual security is not violated in the University of Pamplona headquarters Villa del Rosario and finally strategies were proposed in the regulation of computer crimes for prevention and sanction.

Problem Statement and Justification

The variant technological evolution in the last decades has brought with it the new computer and communication technologies, which have produced a necessary change in the past societies giving rise to this new digital era, in which man seeks the development of his capacity and greater access to information from anywhere in the world, which leads to modify and produce changes in human thinking and the means of social interaction. All this integration of technology with everyday life develops hand in hand with the emergence of a new digital environment, a medium in which each person receives, transmits and obtains information daily, this medium are the social networks in which physical space and time have been modified by cybernetic communication networks that allow processing information and transmitting it in real time from anywhere on the planet generating large information resources in the form of images, text, graphics and sounds. All of this has consequences in multiple spheres since these networks have replaced social space with virtual space.

Today they are presented in so-called social networks, in which computer crimes can be established, it is necessary to know punctually

each of the concepts that cover this subject, to clearly understand which of the activities and events develop the people who are part of these networks, who could be legally sanctioned for concurring in acts that injure the rights and freedoms of individuals and organizations. And so on, as well as objectively managing to direct a country's regulations towards the control and legal restriction of these networks in order to provide all their users with the specific legal tools to defend themselves, prevent and denounce this degrading digital environment.

How do computer crimes affect people's fundamental rights?

General objective

Analyze the regulation of computer crimes through the impact on the fundamental rights of individuals so that their individual, collective security is not violated at the University of Pamplona headquarters Villa del Rosario.

Specific objectives

Recognize the Colombian normative framework for the regulation of computer crimes through the penal code.

Categorize computer crimes through the impact on the fundamental rights of individuals so that their collective individual security is not violated at the University of Pamplona headquarters Villa del Rosario.

Propose strategies in the regulation of computer crimes for prevention and sanction.

The main reason for this project is to establish if there is a legal space that covers this issue of global controversy, the guidelines and follow-ups that can be applied for an effective solution, one of these would be the enactment of all the information related to this so that people in general have knowledge of this subject so relevant that it greatly affects our time because it goes hand in hand with technology, which is useful but at the same time dangerous and most people who use it do not know the risks to which they are exposed by trusting their privacy in an electronic device.

Frame of reference

Regulation in Colombia of computer crimes, in the political constitution.

All persons have the right to their personal and family privacy and to their good name, and the State must respect them and ensure that they are respected. Likewise, they have the right to know, update and rectify the information that has been collected about them in data banks and in the archives of public and private entities. In the collection, processing and circulation of data, the freedom and other guarantees enshrined in the Constitution shall be respected. Correspondence and other forms of private communication are inviolable. They may only be intercepted or searched by judicial order, in the cases and with the formalities established by law. For tax or judicial purposes and for cases of inspection, surveillance and intervention by the State, the presentation of accounting books and other private documents may be required under the terms established by law [3].

Political Constitution. Everyone is guaranteed the freedom to express and disseminate their thoughts and opinions, the freedom to inform and receive truthful and impartial information, and the freedom to establish mass media. They are free and have social responsibility. The right to rectification under fair conditions is guaranteed. There shall be no censorship.

Articles 15 and 20 provide sufficient support for the legislator to enshrine norms aimed at developing what are known worldwide as computer-related crimes. These articles embody an initial idea from which a new regulation can be formulated in accordance with the advance of technology and communications to provide legal security in the use of social networks in the face of computer crimes.

The essential purposes of the State are: to serve the community, promote general prosperity and guarantee the effectiveness of the principles, rights and duties enshrined in the Constitution; to facilitate the participation of all in the decisions that affect them and in the economic, political, administrative and cultural life of the Nation; to defend national

independence, maintain territorial integrity and ensure peaceful coexistence and a just order. The authorities of the Republic are instituted to protect all persons residing in Colombia in their life, honour, property, beliefs and other rights and freedoms, and to ensure the fulfilment of the social duties of the State and individuals. Jurisprudential aspects The high corporations whose functions include administering justice and ensuring that the legal system does not threaten the constitutional charter have not had a notorious jurisprudential activity on the issue of so-called computer crimes, since they have not produced guidelines or strong jurisprudential lines and this is due to the absence of norms that are in tune with the technological technological legal environment related to computer crimes in the penal code and Law 1273 of 2009: The Colombian penal code in chapter VII of the second book of title III: crimes against individual freedom and other guarantees, deals with the violation of privacy, confidentiality and interception of communications: Article 192. Illicit violation of communications. Offering, sale or purchase of an instrument capable of intercepting private communication between persons. Article 194. Disclosure and use of confidential documents. Abusive access to a computer system. Illegal violation of official communications or correspondence. Illegal use of communications networks. These articles are consistent with article 357: "damage to works in communications services, energy and fuels.

This law and legal framework has become an important contribution and a very effective instrument for public and private entities to face computer crimes, with definitions of procedures and information security policies; and, consequently, with the criminal actions that can be brought against persons who incur against the actions typified in the norm. With it, Colombia is located at the same level as the member countries of the European economic community, which expanded the international level of legal agreements related to the protection of information and computer resources of the countries, through the "cybercriminality" agreement, signed in Budapest Hungary in 2001 and in force since July 2004. With the legal developments so far the degrees about "the protection of information and data and the integral preservation of the systems that use information and communication technologies", the organizations can protect part of their integrated information systems: data, processes, policies, personnel, entries, exits, strategies, corporate culture, ICT resources and the external environment, so that, in addition to contributing to and ensuring the characteristics of the quality of information, it incorporates the administration and control of the concept of integral protection. thanks to this typification of the crime, they can be applied to the norm in order to later demand a sanction and thus have a legal framework applicable to the different conducts that are occurring in the social networks that violate and affect the rights of the different users" [5].

International Background

Mayer [6], propose that recognizing an interest of these characteristics is justified if such crimes, in addition to affecting the software of a computer system, involve the use of computer networks. In order to define its juridical good, the study reflects on the functions of computer systems for the free development of the individual and the institutions that are at its service in a democratic State governed by the rule of law [6]. The study examines the functions of computer systems for the free development of the individual and the institutions that are at its service in a democratic State governed by the rule of law.

Trejo [7], presented the computer crimes that can be considered as electronic crimes, so serious that they can become a generic problem for the advancement of computer science. However, it can involve crimes as serious as theft, falsification of documents, fraud, blackmail and embezzlement of public funds. A very common example is when a person comes to steal information and cause damage to computers or servers that may come to be absolutely virtual because the information is in digital form and the damage becomes bigger and bigger. Many of the people who commit this type of computer crimes have different characteristics such as the ability to handle different computer systems or the performance of work and tasks that facilitate access of a simple nature. It can also be defined as any culpable action by the human being is somehow or other leads us to cause harm to people who do not necessarily benefit from different types of computer

management since the criminals who do this type of crime are taking away the possibility of seeing everything in a very different way and by different I mean to see it in an original way without taking anything away or without removing it from the place where it was always kept [7].

Salvadori [8], express that the types of sanctions and actions are not very clear and individuals are not aware of all this event to a large extent, this is the main reason that people are victims of this degrading virtual world.

National Background

Alvarado analyzed [9], the legal aspects of using the two main social networks in Colombia such as facebook and twitter. Through a qualitative descriptive approach and documentary analysis we find results associated with the responsible use and connection of users in social networks and their relationship with the violation of Colombian regulations in which computer crimes are found, the protection of information and data, slander and libel, cyber-bullying and copyright [9].

For Franco [10], social networks have extrapolated interpersonal connections from the physical plane to the cyber plane. In these, users share photos, experiences, and even personal data, which have been used by "cybercriminals" to commit economic crimes. Hand in hand with these, the presentation of other crimes has been evidenced. The flexibility and precarious surveillance of these social networks have given rise to cases of slander and libel among users, affecting their right to honor and privacy. In theory, the State, in its capacity as owner of the criminal action, should prosecute these crimes [10].

Rodríguez [11] analyzed the computer crimes present in social networks in Colombia for 2011 and their regulation. "Cybercriminals travel through the virtual world and make increasingly frequent and varied fraudulent incursions, such as unauthorized access to information systems, computer piracy, financial fraud, computer sabotage, child pornography, among others. To deal with them, however, the difficulty of discovering them, several countries have set up a specialized judicial system that allows them to be prosecuted and punished. Colombia made some progress on this issue with Law 1273 of 2009, which implements a new legal asset called "the protection of information and data," and integrally preserves systems that use information and communication technologies, among other provisions. In order to conclude that the new criminal practices in Colombia are at the hand of the application of technological advances, but in spite of this in Colombia there are legal bases from which it is possible to begin to combat the different modalities of computer crimes, analyzing and interpreting the existing norm to identify its scope, thus obtaining elements of judgment to develop policies and strategies in this subject. [11].

Today, information technology is present in almost all fields of modern life. With greater or lesser speed, all branches of human knowledge surrender to technological progress and begin to use information systems to perform tasks that in the past were performed manually. We live in a rapidly changing world. Before, we could be certain that no one could access information about our private lives. Information was just a way of keeping records. That time has passed, and with it, what we might call intimacy. Information about our personal lives is becoming a highly valued commodity for companies in today's marketplace. "The explosion of the computer and communications industries has allowed the creation of a system, which can store large amounts of information about a person and transmit it in a very short time. More and more people have access to this information, without legislation being able to regulate them" [12].

According to Grisales [13], dogmatic analysis of Theft behaviour by computer and similar means (Art.269I) and Non-consensual transfer of assets (Art. 269j) Law 1273 of 2009. (2013) Eafit University, Medellín, Antioquia. For this reason, it led the author to conduct a dogmatic study of both punishable conducts, taking as a reference the hundreds of cases that enter the offices of the Medellín prosecutors' offices every month. Many of these cases were analyzed in order to illustrate in a clear, simple and comprehensible manner the judges, prosecutors, judicial police officers,

lawyers, rights students and all those who want to know the broad and complicated world of computer crimes in Colombia from the legal standpoint [13].

Regional Background

Granados and Parra [14], refer to the crime of theft by computer that is typified in Article 269I of Law 1273 of 2009 and its applicability in the Judicial District of Cúcuta in the period 2012 - 2014. In Colombia, computer criminals have specialized mainly in theft through computer means, which is the most common computer crime in the country. The city of Cúcuta has not escaped from this, where citizens have also been affected by this type of crime in recent years [14].

According to Castillo et al. [15], information and data protection as a computer crime in Colombia: criminal sanctions in Cúcuta. They established whether Law 1273 of 2009 contributes to the improvement of the security of the information systems that are created by computer companies and that according to national and international standards have so little security. The first chapter analyzes the advantages and disadvantages of Law 1273 of 2009, the second chapter analyzes the implications of this law, the third chapter analyzes the criminal types that were created, and finally, the last chapter analyzes the opinion of the managers or administrators of the computer companies in Cúcuta with respect to Law 1273 of 2009, according to an applied interview type instrument [15].

Theoretical framework

The computer expertise and digital evidence in Colombia, within this speaks of the violation of personal data on page 248, the operator holds a right to administer the information. As such, it has the protection conferred on it, in others, by database copyright laws [16].

Colombian regulations and legislation in relation to computer-related crimes are not present to a great extent in positive law, but there are specialized entities for their regulation and investigation. Criminal Code, Law 599 of 2000.

The Manual of Computer Crime in Colombia. Dogmatic analysis of Law 1273 of 2009. It analyzed the computer crimes described in Law 1273 of January 5, 2009, which attempt against the legal good called "of the protection of information and data"; For this purpose, the concept of legal property in crimes against information and data is defined, its classification is made, the general aspects of the objective and subjective part of the criminal types of such punishable acts are indicated, the objective part of unfairness of each of the same and of some contests of punishable acts is dogmatically analyzed, and the circumstances of modification of the penalty and of the referred crimes are explained [17].

Materials and methods

The research has as its quantitative pproach ollowing the methodology of Hernandez et al. [18] "uses data collection and analysis to answer research questions, relies on numerical measurement, counting, and frequently on the use of statistics to accurately establish patterns of behavior in a population" (p.5), non-experimental quantitative research [18]. The design of research is descriptive-propositive according to Tamayo (2004) is that which comprises the description, recording, analysis and interpretation of the current nature, composition or processes of phenomena. This approach works on the realities of the facts and their fundamental characteristics, to present us with a correct interpretation and to establish strategies. (p. 54) [19]. The non-probability sampling is carried out by the criterion, judgment and decision of the researcher to choose the elements in a subjective way or criteria not based on chance random sampling is found to access the information needed [20]. The sample is 100 students from the University of Pamplona and a questionnaire containing 10 items was applied.

Results and Discussions

The sample was 100 students from the University of Pamplona of Villa del Rosario, the computer crimes questionnaire was applied.

Table I. Categorization

CATEGORIZATION	ITEMS
Social Networking	1,5,8,9
Information in the criminalization of computer crimes	2,3,10
Virtual Thefts	4,6,7

Table II. Category: Social Networks

Category: Social Networks		
ITEMS	NO	YES
1.Has anyone ever accessed your social networks without prior consent?	82%	18%
5. Has anyone violated their personal integrity through social networks?	83%	17%
8. Have you seen how someone else's privacy is exposed by the mishandling of information, photos, videos, etc., on social networks?	16%	84%
9. Has anyone posted their personal information on the Internet?	83%	17%

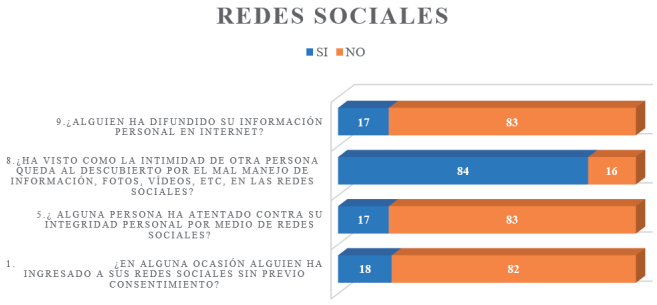


Figure 1. Category: Social networks

1. 82% of students responded that they have not entered their social networks without prior consent; with 18% choosing the option Yes.

5. 83% of the students answered that No, they have attempted against their personal integrity through social networks; with 17% that chose the option Yes.

8. 84% of the students responded that Yes, they have seen another person's privacy exposed by the mishandling of information, photos, videos, etc., on social networks; with 16% that chose the No option.

9. 83% of students responded that No, Someone has disseminated their personal information on the Internet; with 17% who chose option S.

Table III. Category: Information on the penalization of Computer Crimes

Category: Information on the penalization of Computer Crimes		
ITEMS	NO	YES
2. Are you aware that there is a penalty for computer crimes or abusive access?	26%	74%
3. Do you know where the penalty is?	69%	31%
10. Would you like more information on cybercrime and information on its prevention and punishment?	5%	95%

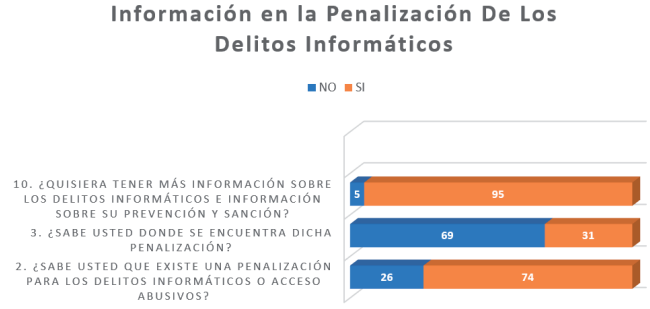


Figure 2. Category: Information on the Penalization of Computer Crimes

2.74% of students responded that If You Know There Is a Penalty for Computer Crimes or Abusive Access; with 26% choosing the No option.

3. 69% of students answered No, they know where the penalty is; with 31% choosing Yes.

10. 95% of the students responded that Yes, they would like to have more information about cybercrime and information about its prevention and sanction; with 5% choosing the No option.

Table IV. Category Virtual Thefts

Category Virtual Thefts		
ITEMS	NO	YES
4. Do you have banking applications on your mobile?	52%	48%
6Have you been a victim of theft by virtual means?	89%	11%
7. Do you know people who are victims of virtual thefts?	46%	53%

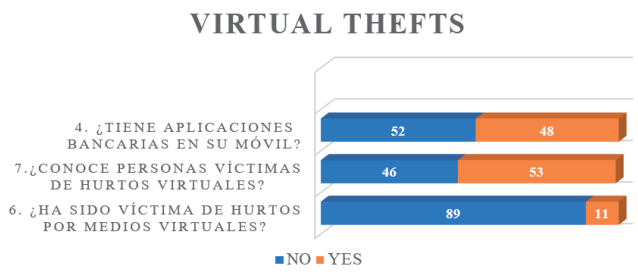


Figure 3. Category Virtual Thefts

4. 52% of the students answered No, they have banking applications on their mobile; with 48% choosing the Yes option.

6. 89% of the students responded that No, they have been victims of theft by virtual means; with 11% that chose the option Yes.

7. 53% of the students responded that Yes, they know people who are victims of virtual theft; with 46% who chose the No option and finally a student, they did not choose any of the response options.

Analysis

In the study sample with the students of the University of Pamplona Villa de Rosario.

Category Social networks; 18% of the students respond that on some occasion someone has entered their social networks without prior consent. 17% of the students responded that Yes, they have attempted against their personal integrity through social networks. 84% of the students responded that Yes, they have seen how the privacy of another person is exposed by the mishandling of information, photos, videos, etc., on social networks. 17% of students responded that Yes, Someone has spread their personal information on the Internet.

Category: Information on the criminalization of computer crimes. 74% of students responded that Si Saben that there is a penalty for computer crimes or abusive access. 31% of students responded that Yes, they know where the penalty is. Ninety-five per cent of students responded that Yes, they would like to have more information about cybercrime and information about its prevention and sanction.

Category: virtual theft. 48% of the students responded that Yes, they have banking applications on their mobile. 11% of the students responded that Yes, they have been victims of theft by virtual means. 53% of students responded that Yes, they know people who are victims of virtual thefts.

Proposition

• The increase of social networks and digital communication platforms, such as Tinder or Snapchat, WhatsApp. The boom in the use of technology in practices such as grooming, sexting or cyberbulling. Students do not know how to react to computer crime. Then the authorities have all the legal and digital mechanisms to investigate cyberbullying or cybercrime. Orientations for formative encounters on cybercrime with learners and educators at Unipamplona:

- Reporting to the virtual CAI or police cyber center, which has a service to report computer crimes and theft of mobile equipment.

- If images, sensitive data, personal data are published without the victim's authorization, a report must be made to the Public Prosecutor's Office for the crime of violation of personal data.

- If the harassment is related to an abusive access to an email account, a cell phone or the profile on a social network, the act can be reported to the Attorney General's Office, as it could be the crime of abusive access to a computer system.

- If the harassment involves other behaviors such as psychological abuse or offenses, it can also be reported for the crimes of slander and libel.

- Additionally, a complaint can be filed with the Data Protection Office of the Superintendency of Industry and Commerce, which has the function of protecting the personal data of Colombians.

- If the cyber-bullying involves a minor, the authorities must be consulted and it must be remembered that there is special protection for minors, such as the Code of Childhood and Adolescence and the laws against child pornography. There are sites like "Te Protejo" that focus on the prevention and protection of minors.

- In order to prevent cyberbullying, it must always be assumed that as little information as possible must

be provided that could lead to digital bullying. It is recommended not to share intimate photographs, or sensitive or personal data that could lead to a person being compromised.

- Currently there are platforms such as Snapchat or Strings, which delete the photo after the person has seen it. There are chat applications that offer more privacy than the usual WhatsApp or Skype. Darkroom, for example, offers a secure chat and deletes conversations after they are read. Others offer encryption features, such as telegram or cryptocat which is under restructuring.

- The Brazilian company Sikur began offering a basic version of chat and encrypted mail free of charge for different devices. Likewise, for secure calls there are applications such as signal, which encrypts calls through an application.

- In cell phones or secure phones, such as granithephone or blackphone. In several countries, government officials already use these devices to protect their communications.

- In the procedural system, the way in which evidence is obtained, stored and presented is the most important part of a digital harassment lawsuit. Many of the harassment cases in Colombia have been declared null and void for lack of evidence, or because the victim does not collect evidence correctly and this affects the integrity of the information.

- Preserving information correctly is perhaps the most important thing you can do to defend yourself from cyberbullying. Evidence can now be retrieved from all types of mobile devices such as computers or websites. What is customary in this type of cases is to secure the evidence with the use of digital and electronic signatures such as algorithms such as hash or Md5, which can certify the integrity of the information.

- It is not the same to collect a digital proof of a device turned on or with active programs or processes than of an electronic device that is turned off. Depending on this, and the type of equipment, different procedures can be performed. One of the most common is to make a mirror copy, so that, in this copy, which is faithful to the original, all analyses and tests can be carried out without affecting the integrity of the information.

- There are several methodologies for the survey of digital information. An example is that offered by the international standard ISO 27037-2012, which gives guidelines for the different phases of analysis, collection and acquisition of digital evidence. A document that I recommend, where the subject can be deepened, is the guide of the department of justice programs.

- Metadata also plays an important role. These are defined as the data within the data, which helps to establish information such as the location of a photo, the camera with which it was taken, date and time, type of file, among other aspects.

- Protecting the evidence properly or seeking computer forensic advice is the best thing a victim of digital harassment can do. The goal is to protect digital evidence, and help you expose it as well as possible in a criminal complaint.

- The best way to avoid cyberbullying is mistrust. It's not about becoming paranoid, let alone moving away from electronic media. The best prevention is to be alert: review everything we do on the Internet, how we share information and with whom we do it.

- Don't give sensitive personal information to sites you don't know, create different email accounts to register on social networks, and even consider using names different from yours. Search for your name on Google or search engines on a regular basis, in case there is an unwanted leak. In short: take care of your personal data.

- And always remember that sharing information with sexual content makes others take advantage of it against you [21].

Training sessions are important to guide learners through computer crime prevention strategies and case management strategies involving the university psychologist. For this reason, institutions, together with parents, have a role in training students to handle virtual media responsibly.

Conclusions

It is important for students at the University of Pamplona to provide information and guidance through training meetings on the subject of computer crimes such as the prevention of fraud or theft, mistreatment and intimidation that occurs on social networks and mobile systems in order not to be victims or victimizers in the interaction of computer tools (ICT).

Social networks are the center of intimidation that violate fundamental human rights and must be resolved to the constitutional provision to restore the rights of those affected in the good name, honor, potential damage caused to the cybernaut or the person, being a victim of harassment, abuse and theft.

It is significant to implement strategies of formative encounters based on the prevention of computer crimes and, secondly, to develop case study strategies in the responsible handling of computer tools and communication (ICT) with university students to promote awareness and culture in the network or ICT in the regulation of web content, both for the volume of data, the number of users and problems of jurisdiction; a key point in the coexistence of the virtual society.

Acknowledgements

Thanks to the student community of the University of Pamplona, Villa del Rosario

References

[1] Ley 1273 de 2009 (artículo 2691), artículo 240 de la Ley 599 de 2000.

[2] J. Ojeda-Pérez et al., "cuad. contab. / Bogotá, Colombia", vol. 11, no. 28, pp. 41-66, 2010.

[3] Constitución política de Colombia. Editorial legis S.A. 2006.

[4] Ibidem.

[5] Código penal, (L. 599/2000). Editorial legis S.A.

[6] L. Mayer, "El Bien Jurídico Protegido En Los Delitos Informáticos", *Revista Chilena De Derecho*, vol. 44, no. 1, 261-285, 2017.

[7] A. C. Trejo et al.,"La Seguridad Jurídica frente A Los Delitos Informáticos AVANCES", *Revista de Investigación Jurídica*, vol. 10, no. 12, 2015.

[8] I. Salvadori, "La regulación de los daños informáticos en el código penal italiano", *Revista de Internet, Derecho y Política*, vol. 16, pp. 44-60, 2013.

[9] M. Alvarado, "Aspectos legales al utilizar las principales redes sociales en Colombia", *Universidad Pedagógica y Tecnológica de Colombia*, vol. 8, 2017. doi: 10.22335/rlct.v8i2.315.

[10] A. Franco, "Las redes sociales y los delitos de injuria y calumnia en Colombia", Trabajo de Grado. *Universidad Católica de Colombia. Facultad de Derecho*, 2017.

[11] J. Rodríguez-Arbeláez, "Análisis de los delitos informáticos presentes en las redes sociales en Colombia para el año 2011 y su regulación", 2014. bdigital.ces.edu.co

[12] J. Rodríguez, "Análisis de los delitos informáticos presentes en las redes sociales en Colombia para el año 2011 y su regulación", 2012.

[13] G. Pérez, "Análisis dogmático de las conductas de Hurto por medios informáticos y semejantes (Art.269I) y Transferencia no consentida de activos (Art. 269j) Ley 1273 de 2009", *Universidad Ea it*, 2013.

[14] R. Granados and C. Parra, "El Delito De Hurto Por Medios Informaticos Que Tipifica El Articulo 2691 De La Ley 1273 De 2009 Y Su Aplicabilidad En El Distrito Judicial De Cucuta En El Periodo 2012- 2014", 2016.

[15] L. Castillo, B. Blanco and R. Pérez, "La protección de la información y los datos como delito informático en Colombia: sanciones penales. Universidad Libre – Seccional Cúcuta", *Trabajo de Grado Universidad Libre, Seccional Cúcuta*, 2010.

[16] R. Granados and A. Parra, "Los autores referencian, el delito de hurto por medios

informáticos que tipifica el Artículo 269I de la Ley 1273 de 2009 y su aplicabilidad en el Distrito Judicial de Cúcuta en el período 2012 - 2014", 2016.

[17] J. Cano, "El peritaje informático y la evidencia digital en Colombia. Universidad de los Andes, facultad de derecho", *Ediciones UNIANDES*, 2010. http//:ediciones.uniandes.edu.co

[18] R. Hernández, C. Fernández and P. Baptista, "Metodología de la Investigación", *Bogotá: McGraw Hill*, 2008.

[19] T. Tamayo, "El Proceso de la Investigación. México", *Limusa*, pp. 54, 2004.

[20] J. Hurtado de Barrera, "Tercera Edición, Fundación Sypal: Caracas. (Parte II, Capítulo 3 y 4)", 2010.

[21] G. Realpe Delgado: CEO de Cloud Seguro y columnista de ENTER.CO.