RCMOS – Multidisciplinary Scientific Journal O Saber.
ISSN: 2675-9128. Sao Paulo-SP.

Cybercrime and the difficulty in applying appropriate measures due to the lack of legislation in combating crimes committed in the virtual environment

Cybercrime and the difficulty in applying appropriate measures due to legislative lack in combating crimes committed in the virtual environment

Ediná de Souza Meira[33]
Solange Barreto Chaves[34]

Submitted on: 05/20/2022
Approved on: 05/20/2022
Published on: 05/21/2022 v. 2, no. 1, Jan-Jun. 2022
DOI: 10.51473/rcmos.v2i1.301

SUMMARY

The present study aims to analyze the evolution of cybercrimes and the difficulty in identifying those responsible. The aim is to investigate the causes associated with the practice of cybercrimes, such as criminal authorship and the collection of evidence, as well as demonstrating the vulnerability of Brazilian legislation in the face of criminal practices in the virtual environment, observing the fragility of specific standards in the definition of some crimes. and in the application of a sanction that corresponds to the illicit acts committed. To this end, this research will carry out a bibliographic analysis with materials published in periodicals, magazines, books and electronic networks. In addition to consulting government websites to address the aforementioned laws.

Key words: Crimes Cybernetics. Internet. Legislation. Virtual Crimes. Failure Legislative.

ABSTRACT

The present study aims to analyze the evolution of cyber crimes and the difficulty in identifying those responsible. It seeks to investigate the causes associated with the practice of cyber crimes, such as criminal authority and the collection of evidence. Demonstrate the vulnerability of Brazilian legislation in the face of criminal practices in the virtual environment, observing the fragility of specific norm in the definition of some crimes and in the application of sanctions that correspond to the illicit practiced. Therefore, the present research will carry out a bibliographic analysis with materials published in periodicals, magazines, books and electronic networks. In addition to consultations with government websites to address the aforementioned laws.
Keyword: Cyber Crimes. Internet. legislation. Virtual Crimes. Legislative Insufficiency

1. INTRODUCTION

The technological development of humanity has brought with it several transformations, the most significant of which is the emergence and expansion of the Internet, and consequently covering the entire planet. Despite the important role that the internet plays in human life, not everything is perfect, as individuals now seek to obtain some benefit, whether legally or illegally.

Therefore, criminal activity is an alarming fact, even when it comes to the applicability of the law, since in most cases identifying criminals is hard work, so they tend to remain anonymous, and consequently go unpunished.

In this case, as Machado (2017, p.07) says, "the lack of an incriminating standard for some conduct practiced by through computer systems, make it difficult to apply an adequate sanction to those who practice illegal conduct".

That said, the research is analyzed using bibliographical research methodology through books, materials

[33] Law student at Faculdade Santo Agostinho de Vitória da Conquista.

[34] Graduated in Law from the State University of Southwest Bahia – UESB (2018); Post graduate in Administrative Law from Estácio de Sá (2019); Postgraduate in Higher Education Practices from Faculdade Santo Agostinho – FASAVIC (2022); Postgraduate student in D. Civil and Proc. Civil by LEGALE (2022); Master's student in Law at the Catholic University of Salvador (2022 – 2024); Professor at Faculdade Santo Agostinho in the subjects of Civil Procedure III and IV, Tax Law II, Legal Service I and II and Legal Entrepreneurship. Email: solange.chaves@vic.fasa.edu.br

published in periodicals, magazines and electronic networks. This text addresses issues about digital law with a focus on cybercrime and the difficulty in applying appropriate measures due to the lack of legislation in combating crimes committed in the virtual environment.

2. CYBER CRIMES

Cybercrime or cybercrime (in English,*cybercrimes*) is any and all illicit activity committed on the internet, through electronic devices, such as computers and cell phones. Practices range from the spread of viruses to attacks on the operating systems of companies and private individuals. In this way, offenders are able to access confidential information and data, with the intention of harming the individual.
In this scenario, computer crimes began even before the emergence of the internet. However, with the arrival of the internet, there are different forms of interactivity between people, in the same way that virtual crimes arise.

2.1 Species

When it comes to types of crimes, those that occur most frequently are those against honor, "crime of defamation, crime of slander, crime of insult" and there are crimes of: Invasion of privacy, Electronic espionage, Virtual fraud, Pornography children, against intellectual property and fraud. Quickly conceptualizing it as follows:

- Invasion of privacy: illegal access to user information occurs, with the possibility of leaking information;
- Electronic espionage: through software that improperly spies on information on servers;
- Virtual fraud: the conduct refers to the modification, alteration or tampering of a data processing system or electronic program;
- Child pornography: there is the dissemination or sale of erotic material involving children or adolescents;
- Against intellectual property refers to materials with copied data that circulate freely;
- Swindle: the intention is to acquire illicit benefits for oneself or for other purposes;

There are other crimes that can still be listed, however, statistically it is not appropriate to highlight them in the research carried out, focusing only on an analysis of the most recurrent ones.

2.2 Legislation

Regarding criminal legislation, Ramos (2017, p. 38), highlights that "the Convention on Cybercrime does not dictate rules, but rather provides guidance on the topic, leaving it up to each country to create its own specific legislation".
Thus, it will allow governments to develop their laws and regulations to identify and punish criminals based on the particularities of their cybercrime legal systems.
Today, the Brazilian legal system has some rules to protect matters related to the virtual environment, but it still does not fill the legislative gap on the issue in the country.

2.3 From the provisions of Law No. 12,737, of 2012.

Due to the time in which it was written, the Brazilian Penal Code did not include articles to deal with crimes in the digital environment, thus, in its article 1, the Penal Code informs that there is no crime, without prior legal definition, thus the crimes Virtual networks only began to be treated more prominently from 2012 onwards, when in November of the same year, with the enactment of Law No. 12,737, the Penal Code was amended, adding articles 154-A and 154-B and modifying the text of articles 266 and 298 for the criminal classification of computer crimes.

The ratification of Law No. 12,737/12, which is popularly known as the Carolina Dieckmann Law, took place shortly after the actress had several intimate photos published due to an invasion of her personal computer, an event that had national repercussions.

Law No. 12,965, known as the Marco Civil da Internet, establishes principles, guarantees, rights and obligations for the use of the Internet in the country, as well as guidelines for the functioning of the Union, the States, the Federal District and municipalities on this topic. Therefore, private data and information that exists on a website or social network can only be accessed through a court order.

With the beginning of the Marco Civil da Internet Law, one of the main innovations is the removal of content from the air, the deletion of this content takes place through a court order, except cases involving revenge pornography, as victims can request the removal of the content directly from the website or service containing the content.

2.4 From aggravation to crimes of computer device violation - Law 14,155/2021

Law No. 14,155, of 2021, amends the Penal Code, making the penalties harsher for device hacking, theft and fraud occurring in the digital world, regardless of whether it is connected to an internet network or not.

The law changes and creates aggravating circumstances in the wording of some articles of the Penal Code that deal with computer crimes, with an increase in the sentence from four to eight years, ceasing to be a detention regime and changing to imprisonment, for thefts committed using these devices. , regardless of whether the devices are connected to the Internet, use passwords or even another security mechanism.

However, with regard to identification, Alves considers that:

> There is great difficulty in punishing cyber crime offenders, taking into account the increasing increase in this type of crime in our country and the lack of laws, thus becoming a legal problem as well as a serious social problem. (ALVES, 2018, p. 3).

And according to Maia (2017), the civil framework is based on three pillars: ensuring network neutrality, protecting the privacy of internet users and guaranteeing freedom of expression, which is why Brazil needs to immediately turn its attention to developing legislation specifically about cybercrimes, given that the Internet has become an integral part of our daily lives. Therefore, it is necessary to aim for the approval of a code to guide all relationships carried out in the digital environment, describing conduct in a simplified way so that they can be easily incorporated into the facts.

3. POSSIBLE INVESTIGATIVE DIFFICULTY IN THE APPEARANCE

Due to the sharp development of information technology, investigators face many difficulties in the cybercrime investigation process. However, despite some challenges in police investigation, many solutions are being sought, such as specific laws and better training of agents responsible for criminal prosecution to keep up with the continuous development of technology and the advent of new technologies that accompany it. Some computer crimes are often carried out based on computing experience and strategy. These strategies can be developed by groups of people who generally know each other. These factors make it difficult to figure out who is responsible for the behavior.

Another notable feature, especially in computer crimes involving fraud or theft, is that they are generally carried out very quickly. In some cases the victim does not even realize that they have been attacked, in other cases they only realize when certain events occur, such as when a website *web*is changed during use, or when it receives a *email* warning.

When such acts are committed on the Internet, the punitive nature has judicial difficulties in identifying the subject, due to insufficient evidence for the composition of the crime and such crimes being committed in a virtual environment.

Today, anyone with minimal technical knowledge can carry out illegal acts using a computer. However, it is believed that criminals in this universe are intelligent, kind and polite people. Furthermore, They consider themselves competent operators of computers and systems, they are adventurous, daring and seek to surpass their knowledge.

In this context, it is important to note that not all cybercriminals are computer experts. Ordinary users only need to know how to use a computer and navigate the Internet to commit crimes such as defamation and pedophilia.

When a computer crime occurs, it is necessary to carry out an investigation in order to provide evidentiary support for future criminal proceedings. Investigative team members have access to a variety of resources during the investigative process.

Just as people have numbers that identify them, such as CPF (Individual Taxpayer Registry), computers and peripherals connected to the Internet are also differentiated by IP addresses. This protocol number is unique and allows machines to communicate on the network.

IP number identification *(Internet Protocol)* brings the possibility of locating criminals, but the only way to control the increase in crimes is the law, due to instituting punishment for illegal behavior.

In addition to legal procedural measures to obtain evidence in cybercrimes, there must be a well-developed scientific police, with qualified and trained personnel in the area of information technology and mastery of new technologies. In addition to access to top-of-the-line equipment, given the high specialization of these activities, they can examine and evaluate the data collected.

Even though several benefits have emerged with the advent of the Internet, new types of crimes have evolved to such a point that the anonymity of the world wide web has contributed to the proliferation of these illicit conducts. The implementation of the internet has led to a substantial increase in the types of virtual crimes, forcing the population and authorities to seek mechanisms to prevent crime and punish criminals.

The investigation to ascertain the authorship of the act is essential for the identity of the perpetrator of the crime, since innocent people can be blamed due to their accounts being attacked, so the intention to punish must fall to those who actually committed the crime, this is the case. Tourinho Filho's position citing Carnelutti:

> The problem of the accused's qualification is of paramount importance, because, in the case of a very personal quality, it cannot be attributed to anyone other than the true culprit. CARNELUTTI teaches with authority (leccciones, cit., v. 1, p. 195).

In this sense, the Civil Police and the Federal Police, which are the public security bodies responsible for investigation, especially the sectors specialized in this type of crimes, need to be properly equipped to effectively and proactively combat cyber threats. In addition to a strategic program, and being prepared for possible problems similar to the topic discussed.

4. TESTS

Law has the function of regulating legal relationships between individuals, as it aims to protect the legal assets of this relationship, whether common assets or non-habitual assets.

And when the subject is the evidentiary elements, it becomes one of the most important topics in the process in the legal system, its purpose is to convince the judge of the sentence of fact. In this sense, Norberto Avena adds:

> Evidence is the set of elements produced by the parties or determined by the judge aiming to form a conviction regarding acts, facts and circumstances. [...] The production of evidence aims to help convince the judge regarding the veracity of the parties' statements in court. (AVENA, NORBERTO, 2017, p. 315)

Still on the subject, Távora and Alencar:

> [...] proof is everything that contributes to the formation of the judge's conviction, demonstrating the facts, acts, or even the law itself discussed in the dispute. Intrinsic to the concept is its purpose, the objective, which is to obtain the conviction of the person who will judge, deciding the fate of the defendant, convicting or acquitting. (TÁVORA E ALENCAR, 2017, p.618).

It is worth noting that in cybercrimes, certain means of proof are more evident, such as the tests that can be carried out on the computer handled by the likely perpetrator. Other possible means of proof would be the interception of emails, breach of confidentiality on social networks such as *Telegram, Facebook, Instagram, Whatsapp*, between others. However, we cannot say that the suspect will be identified, however identification becomes more likely.

Thus, when it comes to proving crimes committed in the virtual environment, great difficulties arise, due to the fact that crimes committed in this area do not usually leave traces, and when they do, most of the time it is not enough to fit into the existing criminal types that deal with of the subject. The conduct must be equivalent

to what is described in the criminal type, and only then will it constitute a crime leading to punishment for the perpetrator.

The evidence has a broad scope, as it not only proves what happens in the network environment, but also provides support for what happens in our everyday lives.

It is necessary to protect those whose privacy and reputation are invaded through fake news, publication of defamatory content, distribution of unauthorized images, etc. Conflict is very common in our daily lives, as more and more people have access to virtual environments, more conflicts occur every day, and the number of lawsuits only increases.

FINAL CONSIDERATIONS

Initially, the concept of cybercrime was developed, where the topics covered are clarified based on an understanding of what is classified as a crime and a record of ongoing crimes.

Soon after, the question is addressed, presenting the entry of new technologies brought about by the globalization process, culminating in the first crimes committed in the digital field. However, in a short period, new types of crimes have emerged, without laws to guide them.

When it comes to types of cybercrime, the most common crimes in this environment were observed. In addition to observing the importance of evidence, as well as the difficulty in investigating evidence that could identify authorship.

It is clear that some laws are emerging to address and support crimes committed in virtual environments, but they are not sufficient, and the fragility of these standards causes an accumulation of unresolved cases. Therefore, the need to draft specific laws becomes more essential every day.

REFERENCES

ALVES, MH dos S.**The evolution of cybercrimes and the monitoring of specific laws in Brazil.**Published in 2018. Available at: https://jus.com.br/artigos/64854/a-evolucao-dos-crimes-ciberneticos-eo- follow-dasleis-especificas-no-brasil.

AVENA, Norberto.**Criminal proceedings.**9th ed. rev. and current. Rio de Janeiro: Forensic; São Paulo: METHOD, 2017.

BRAZIL.**Penal Code.**Brasília: Planalto Site, 1940. Available at: http://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm.

BRAZIL.**Criminal Procedure Code.**Brasília: Planalto Site, 1941. Available at: http://www.planalto.gov.br/ccivil_03/decree-lei/del3689compilado.htm.

BRAZIL.**Constitution of the Federative Republic of Brazil.**Enacted on October 5, 1988. Brasília: Senado Federal, 1988.

BRAZIL.**Law No. 12,737.**Brasília: Site Planalto, 2012. Available: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm.

BRAZIL.**Law No. 14,155.**Brasília: Website Planalto, 2021. Available at: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/lei/L14155.htm

BRAZIL.**Civil Rights Framework for the Internet.**Brasilia: Planalto Website, 2014. Available at: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm.

BRAZIL.**Federal police.**Brasília: Federal Police website. 2022. Available at: https://www.gov.br/pf/pt-br.

BRAZIL.**Federal Senate.**Brasília: Federal Senate website. 2022. Available at: https://www12.senado.leg.br/hpsenado.

MACHADO, TJX**Cybercrime and crime in the computer world.**Fernando Pessoa University. Porto, 2017.

MAIA, TSF**Analysis of mechanisms to combat cybercrime in the Brazilian criminal system**.Federal University of Ceara. Faculty of Law, Law Course, Fortaleza, 2017. Available at: http://www.repositorio.ufc. br/ bitstream/riufc/31996/1/2017_tcc_tsfmaia.pdf.

RAMOS, ED**Cybercrimes:***Evolutionary analysis and Brazilian criminal legislation*.Law Course at the Federal University of Rio de Janeiro. 2017. Available at: https://pantheon.ufrj.br/bitstream/11422/6911/1/EDRamos.pdf.

TÁVORA, Nestor; ALENCAR, Rosmar Rodrigues.**Criminal procedural law course.**12th ed. rev. and current. Salvador: JusPodivm. 2017.

WEND, Emerson; VINICIUS, Higor; JORGE, Nogueira.**Cyber Crimes:***Threats and investigation procedure*. 3rd ed. Rio de Janeiro: Brasport, 2021.