ISSN: 0975-833X

Availableonlineathttp://www.journalcra.com

International Journal of Current Research
Vol. 11, Issue, 05, pp.4190-4196, May, 2019

DOI: https://doi.org/10.24941/ijcr.35484.05.2019

INTERNATIONAL JOURNAL OF CURRENT RESEARCH

RESEARCH ARTICLE

ANALYSIS OF CYBER CRIMES FROM THE PERSPECTIVE OF PROPORTIONALITY: INCONGRUENCES OF THE LAW 12.737/2012

[1]Wagner Matheus Silva Domingues, [2]Iaggo Raphael David, [1,2,3,4*]Stenio Fernando Pimentel Duarte and [1,4]Luciano De Oliveira Souza Tourinho

[1]Independent Faculty of the Northeast – Bahia, Brazil
[2]Public Health Foundation of Vitória da Conquista – Bahia, Brazil
[3]Faculty of Technologies and Sciences – Bahia, Brazil
[4]Faculty of Santo Agostinho – Bahia, Brazil

ARTICLEINFO

Article History:
Received 15th February, 2019
Received in revised form
10th March, 2019
Accepted 07th April, 2019
Published online 30th May, 2019

Key Words:
Computer Crimes, Invasion.
Computer, Privacy,
Law 12,737 / 2012.

ABSTRACT

With the approval of law 12.737 / 2012, the crime of invasion of computer devices in Brazil was typified. The approval of the law by the National Congress and occurred after the repercussion given to the subject after intimate photos of the famous actress Carolina Dieckmann, have been released on the internet without his permission. It is a criminal type with many elements open, which need to be limited and clarified for a correct application to concrete cases. The purpose of this study was to analyze the crime brought by article 154-A, and added to the Criminal Code by Law No. 12,737, of November 30, 2012, known as the "Carolina Dieckmann Law", through which it was possible to verify existing ambiguities in the caput of that article, as well as the penalty imposed which does not comply with the principle of proportionality and renders the law ineffective.

**Corresponding author:*

Citation: Wagner Matheus Silva Domingues, Iaggo Raphael David, Stenio Fernando Pimentel Duarte and Luciano De Oliveira Souza Tourinho. **2019.** "Analysis of cyber crimes from the perspective of proportionality: incongruences of the law 12.737/2012", *International Journal of Current Research*, 11, (05), 4190-4196.

INTRODUCTION

This work has as its theme Law 12,737, known as the "Carolina Dieckmann Law", which changed the Brazilian Penal Code by criminalizing cybercrimes. A law that had its procedure accelerated in the National Congress due to the exhibition on the internet, of photographs of the actress. The typification of the virtual crime in Brazil is recent, but crime is recurrent and old in the country. Thus, the Law No. 12 737, becomes a milestone in the quest to fighting this type of crime, aiming to give greater protection to privacy. However, some lawmakers point out that the ambiguity of the wording together with (non) compliance with the Principle of Proportionality makes Law No. 12,737 / 2012 ineffective, causing a sense of impunity and legal insecurity before every society. For still beingsubject of several controversies, Law No 12,737 deservesbe studied and understood, given its relevance to the law, as it pertains to your application. Thus, the importance of this topic, which seeks to discuss the gaps left by the legislator in drafting the text of Article 154-A, of said Law, as well as to clarify (in) compliance with the Principle of Proportionality, provides a critical reflection of the current Brazilian scenario, in which criminal laws are created. For the development of the study, the literature review was made. Based on a doctrinal and normative construction, Law 12,737 / 2012, as well as theses, dissertations, doctrines and articles published on the internet, the study addresses historical, conceptual and normative aspects of virtual crimes. It should be noted that, for the development of the present work, in relation to the technical procedures, the bibliographical research was used, which consists of research materials coming mainly from books and scientific articles, but because it is a specific topic, research was necessary of virtual publications,indexed in the database Scielo and Periódicos Capes that deal with the subject in question. Regarding the method of approach, the deductive mode was used, starting from more general theories and laws for the occurrence of particular phenomena.

Considerations on the technological revolution and the internet: According to Soares and Alves (2008), the world has undergone several transformations, among them is the technological revolution that contributed to making the technological resources of communication and information

available to all. Over the years, we have seen that technology has progressed more and more and has gained more and more space. As Queiróz *et al*. (2004) points out, the advent of information technology interfered with men's way of thinking, acting, acquiring knowledge and solving problems. As it evolved in social, economic and scientific relations, it felt the need to reduce geographical barriers, a fact that encouraged, from World War II, the investment in the development of new, faster and more efficient means of communication. In addition, it enabled the storage and processing of an increasing amount of data that gave rise to the New Technologies of Information and Communication (TIC), among which the computer stands out. The computer, according to Castells (2006), was gradually used for professional purposes and despite the high iterativity, it is nowadays one of the largest communication vehicles of the masses, largely used for messaging services, integrating people and creating a globalized social environment.

The first computer language, according to Queiroz *et al.* (2004) only came out in 1956. Named Fortran, this first computer language was developed for the IBM 701 computer. From there, many other computer languages were developed for specific purposes, being used for both business and problem solving mathematical or programming. Since then the evolution of ICT has taken a significant step forward. Several systems have been created, such as "e-mail" services and the "online" group agenda. It is possible to consider the "Internet" as a milestone and one of the most significant advances of the last decades of the twentieth century, since it allowed the creation of several other systems. According to Levy (1999: 5), "new ways of thinking and living are being elaborated in the world from the evolution of informatics. The relations between men, work and intelligence themselves depend, in fact, on the innovations of technological devices of all kinds ", and in particular, computers connected to the Internet. Along with the internet, technological advancement becomes evident, making the computing environments spread geographically and in an organized way, giving data communication an important role. And, all this information exchange and data storage over the internet is becoming available on mobile devices, such as the cell phones, tablets and smartphones of this generation.

Currently, Internet-related ICTs have played a very important role in corporate and social communication, as Vieira (2010) explains. They have evolved very quickly, generating differentiated and sophisticated products and interfering with how we relate to other people, with the things around us, thus creating a new culture and a new model of society. A technological society characterized by the speed of changes in the informational universe and the need for permanent updating of man to follow these changes. The Internet, according to Kotler (1999), has represented unlimited access of the population to information related to goods, products and services of all kinds. According to Ibope / nielsen online (2010), the internet represents the third most widely used vehicle in Brazil, a factor that has influenced the behavior of people and influenced the increase in virtual crimes, a topic that is discussed below.

Computer Crimes: Throughout the history of mankind, man has shown a constant concern to keep track of their lives, initially depicting their daily lives in stones, wood carvings or even charcoal marks on the walls of caves and various scribbles. The walls of history did not only retract the day-to-day doodles, but also facts and animals of the time, as well as counting time and calculations and numerical equations (SILVA, 2003). Of the writings in the caves, one can perceive the difficulty of the man in the area of mathematics, causing that this one looked for means that facilitated and it took to a reliable result. Due to this difficulty of calculations, man was led to technological advancement in the area of computing, however, not only because of the need for agility in mathematical operations, computing ended up rooted in all other interactions of society (SILVA, 2003). Thus, in every society there are practices practiced that bring consequences, whether civil or criminal, and because they are practiced in the computer system, are referred to as 'virtual crimes', 'cyber crimes' or 'computer crimes'. The practice of criminal conduct, such as Albuquerque (2006), tax evasion, counterfeiting, stock-market fraud, investment fraud, breach of business secrets, invasion of privacy often occurs with the use of information technology to them a new *modus operandi*.

According to Finkelstein (2011), despite computer crimes occurring long before the advent of the Internet, it was from the greater access of people to this important communication resource that this type of crime reached higher levels. Terminologies used for crimes or offenses committed through the Internet are not regulated in Brazil. There are several expressions used by criminologists to conceptualize computer crimes, such as cyber crimes, computer crimes, technological crimes, computer crimes, internet crimes, cyber crimes, digital crimes, among others. In this research was used the nomenclature "computer crimes", because it is the term brought by law nº 12.737 / 2012, object of study. In this context, Silva (2003) points out that because of the lack of unanimity in nominating criminal or criminal conduct practiced online, it requires care when using these nominative expressions. That being so, computer crime may be regarded as any typical, unlawful or guilty conduct practiced by a natural or legal person through information technology for the purpose of automatic data processing or its transmission in which a computer connected or not to the worldwide computer network (ROSSINI, 2004). Rosa (2005), in turn defines computer crime as any illegal conduct practiced from data processing via the internet and with the objective of obtaining undue and illicit advantages. Similar to that adopted by Rodrigues (2002).

It should be noted that, unlike real-world crimes, those committed virtually do not have their own characteristics, they do not follow standards, since they do not require physical contact between the attacker and the victim, crime), occurs in virtual environments (without people, government or territory), does not cause violence, and there is no standard for the occurrence of virtual crimes. According to Albuquerque (2006, p. 40), a succinct and precise definition can not be elaborated without doubts as to its purpose or with regard to the very use of the definition that is given to it. The notion of computer crime involves various kinds of crime. One should not adopt a formal, static definition, which can create more confusion than solutions. Furthermore, computer crime does not have territoriality, since it can be practiced anywhere in the world, from anywhere in the world, and can be practiced in one country and partially in another, or even in third countries, so to speak, a in the United States can modify data stored in Brazil, and then transfer them to the United Kingdom with the objective of obtaining an illicit advantage (ALBUQUERQUE, 2006).

Thus the path of crime is often fragmented, originating from different regions of the world, with no borders to prevent crime. On the classification of computer crimes, they can be classified into own and improper. But considering the most varied doctrinal classifications, two types of computer crime can be considered: common and specific. The common ones would be those already predicted as crimes under prevailing criminal law even before the emergence of the Internet, while specific computer crimes concern those committed against legal goods and that do not yet have a defined law to criminalize them (ALBUQUERQUE, 2006).

Also according to the Albuquerque (2006) teaching can be understood as common computer crime improper crimes, and specific computer crimes as crimes themselves. Inappropriate or impure computer crimes are those in which computer devices are not essential to the commission of the crime. That is, they do not depend on such devices to characterize themselves, serving only as instruments for the commission of crimes already typified in Brazilian law, such as, for example, crimes against honor and patrimony that may be committed by other means, not necessarily through the computer environment. In this sense, Vianna and Machado (2013) warn that the mere fact of using a computer to commit a crime does not constitute computer crime. Vianna and Machado (2013) conclude then that the analogy is inadmissible in this case, since in criminal matters to create crimes and commence penalties, the analogical procedure is only allowed in cases of non-incriminating criminal laws, which leads one to understand that it is it is essential to classify virtual crimes in the Brazilian legal system so that there is social control in relation to crimes practiced in the electronic medium.

Own or pure crimes, for once, are criminal conduct that injures legal property intrinsic to computer devices, such as a violation of the data, information or structures attached to it. In this way, it can be said that directly affects the intimacy and privacy of the victim, contained within the computer device itself. In this same thinking, proper are those crimes in which the active subject essentially uses the computer device to violate the data or computer system of the taxpayer, as clarified by Pinheiro and Haiakal (2013). In turn, Sydow (2015, p.88) teaches that "computer crimes of their own are typical unlawful and culpable conduct aimed at reaching a computer system or its data, precisely violating its confidentiality, integrity or applicability." It can be concluded, therefore, that in order to practice the computer crime itself, it is essential to use information technology, because without the use of it, it would not be possible to practice such criminal conduct. This new reality added to the lack of legislation, causes some computer crimes to be considered atypical, which in most cases, their agents become unpunished.

The computer crimes themselves, the focus of this research, are currently represented in art. 154-A of Law 12,737 / 2012 as those that allow the invasion of private operating systems without authorization for the dissemination of virtual plagues, among which are known as "hackers", "thefts", *Spyware, Key loggers*, *Phishing Scam* and that are used to invade systems and computers with the purpose of stealing passwords and propagating viruses or to appropriate the characteristics and personal identifications of another user to impersonate them without having been authorized to do so. Regarding the subjects of the virtual crime, Corrêa (2000) states that all users, as a rule, who use computer devices to access unauthorized information may be considered computer criminals. The perpetrator (the subject who invades the computer system), as well as the victim (person who suffers the attack) are subjects involved in the offense. These delinquents who attack third-party computer systems are the active subjects of crime. Already, the victims, are the pasive. There are several virtual criminals, highly trained and with their own characteristics, since the dissemination of computer devices and the internet makes it possible to commit computer crimes by anyone. Virtual criminals may be nominated as *Hackers*, *Phreakers*, *Crackers*, *Spammers. Hackers* are highly trained users and equipped with computer expertise to access any type of computing device. These users are mostly hired by various companies to develop security mechanisms for and combat any type of unauthorized access in business systems. The *Crackers* are opposed to *hackers,*because although they have the same knowledge about computers, violate security networks and information systems in order to obtain information, confidential data of companies and people, and then market them, expose them or even destroying them (NOGUEIRA, 2008).

The *phreakers* are specialists in fixed or mobile telephony. They act by circumventing telephone systems to obtain free calls and installing telephone handsets to aid in attacks on computer systems (ROSA, 2005), while *spammers* are all users who use abusive methods to send unwanted e-mail to all e-mail boxes. -mails possible (NOGUEIRA, 2008). In 2012, Law 12,737 / 2012, popularly known as the Carolina Dieckmann Law, was the subject of this research and dealt with below, which typifies the crime of invasion of computer devices in Brazil, but has been and continues to be a stage of criticism due to some shortcomings and gaps, more specifically in Article 154-A, which will be analyzed below.

Law Nº 12.737 / 2012 - "lai carolina dieckmann: This legislation appeared in May 2012, from the episode that involved the actress Carolina Dieckmann who had her intimate photos captured improperly after her computer was accessed by crackers. These subjects, through electronic mail and phone calls, tried to extort the victim so that the photos were not divulged. After the frustrated attempt of extortion, the images were widely publicized in the internet, mainly in pornographic sites.

The enormous repercussion caused by this episode ended up accelerating the process of processing the bill in the Chamber of Deputies. Coincidence or not, 2012 was a political year, and this project was carried out as a matter of urgency, as provided in Article 155 of the Internal Rules of the Chamber of Deputies (BRASIL, 1989). The Law, even before it was approved and published, was already known as the "Carolina Dieckmann Act." After the proceedings in the Chamber of Deputies, the bill was presented to the Federal Senate and approved on November 30, 2012. Thus, on December 3, 2012, Law No. 12,737 of November 30 was published in the Official Gazette of the Union of 2012, which typified computer crimes and amended the Brazilian Penal Code. The Law added articles 154-A and 154-B that defines the crime of invasion of computer equipment, and modified the text of articles 266 and 298 of the Penal Code, regarding the interruption of public service or information of public utility and falsification credit or debit card, respectively. It is perceived that the new criminal type brought by Law 12.737 / 12, in its article 154-A, was born with the intention of protecting users from invasions of computer devices, as well as the constitutional values of

privacy and privacy, protected by the Federal Constitution , in art. 5, X, which guarantees the inviolability of the private life, honor and image of the people, also assuring the "right to compensation for material or moral damages resulting from their violation" (BRAZIL, 1988). However, according to Vieira (2002), both the right to privacy and intimacy are indispensable conditions for the realization of human dignity as a fundamental right. There is a variation from person to person. Thus, what may be intimate for one person may not be for another, and should be analyzed on a case-by-case basis. In this context, conceptualizing these terms is not an easy task. The authors find great difficulties in forming concepts about intimacy and privacy because the values existing in society change in time and space, causing oscillations in the content of the right to intimacy, as well as in the privacy (VIEIRA, 2002). However, one can conceptualize the right to privacy as the individual's ability to prevent strangers from interfering in their private and family life, preventing them from accessing their private information, as well as the dissemination of information about this area of existential manifestation of the human being (BASTOS, 2001). The right to intimacy consists in the legal power to subtract from the knowledge of others and to prevent any form of disclosure of aspects of our existence that, according to the prevailing social values are worth keeping under reserve "(SILVA, 1998, p 131). Law 12.737 / 2012, in its article 154-A, deals with conduct that violates privacy and whose material object is information technology. However, due to the acceleration of the project of the said Law, ambiguities arose and criticisms were made by the doctrine, such as the difficulty of interpreting the verb "invade" - core of the type and the elementary ones that complete the typical figure, as well as some constitutional principles which were not duly observed during the creation of the Law. Subject discussed below.

Criticism of the incriminating criminal type provided in art. 154-a of law 12,737 / 2012: The incriminating criminal type brought by art. 154-A, of law 12.737 / 12[1], strongly criticized by the doctrine, applies when the subject invades the computer device without authorization or installs some vulnerability to obtain some kind of advantage.

In other words, the subject of the offense violates the security of the device without the authorization of the owner or installs some*s oftware* that causes a vulnerability, making it possible to obtain the data. Therefore, it is possible to demonstrate several controversial points, which generate ambiguities as to the efficiency of the norm, where inappropriate specialized techniques end up generating a legal impossibility to punish certain behaviors, considering its atypicality. Until the law was created and published, although there were some appropriate criminal penalties in place to punish virtual crimes, there was in fact no specific provision for cybercrime. In art. 154-A, of Law 12.737 / 12, initially analyzing the text of the article, it is possible to highlight the nucleus of the type, the verb *"invade"*, which has the meaning of violating, accessing, entering, without express or tacit authorization of the holder of the computer device. As Reis (2013) disposes of the verb invade has a different meaning from violating or joining, clandestinely, so, judging by the wording of said article, would only configure the offense if the agent entered the device by force.

About the nuclear verb of the criminal type, teaches Blum (2014) explains that this has the idea of entry to force, barrier violation. In this sense, it can be emphasized that the terms "*invade*" and "*have access*", are completely different, because it is possible to have access to certain computing devices without necessarily invading them. The crimes that the art. 154-A intends to restrain, does not occur in an eventual way, but only with the malicious agent acting, there being two means of accessing the data: the first, when the agent physically accesses the computer device; and the second, when the user installs malware on their device, without knowing it, the species of files sent by e-mails, site links, photos, which cause vulnerabilities in the equipment, allowing to conclude that in both cases , the agent did not act with violence, but only with the use of artifice to obtain data. The solution to solve and cover all these crimes would be the substitution of the core of the criminal type, the verb "invade" by "access", since there would be no need for the agent to act with violence, but only by means to obtain the data , demanding more clarification from the legislator about *malware* (REIS, 2013, without paging).

Still, the nuclear verb "invade", despite its variable amplitude, has no specific meaning in the area of Computer Science. It would be more logical to use the verb "access", already consecrated in the doctrine, since in this branch of Computing is understood as access to the action of reading, writing or executing data stored in computing devices. In a technical language, Vianna (2003) in defining these terms concludes that the verb to access in art. 154-A, of Law 12.737 / 12, is directly related to the specific purposes of acting that compose this incriminating criminal type. When analyzing the elementary normative *"through improper breach of security mechanism"* it is realized that the invasion must occur through the violation of some security mechanism, already listed in previous topic, to be criminalized. Thus, if there is no normative element of the type *"security mechanism"*, the conduct will be characterized as a criminal indifference. In this sense, the most correct would be, if the rule had limited to the phrase *"by improper breach"*, because, in this way, it would cover any type of unauthorized violation of the computing devices, or, as normative text brings, the violation of any "Computer device", regardless of whether or not there is a security mechanism, and regardless of whether or not this mechanism has been violated.

[1]Art. 154-A. Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita:
Pena - detenção, de 3 (três) meses a 1 (um) ano, e multa.
§ 1º Na mesma pena incorre quem produz, oferece, distribui, vende ou difunde dispositivo ou programa de computador com o intuito de permitir a prática da conduta definida no caput.
§ 2º Aumenta-se a pena de um sexto a um terço se da invasão resulta prejuízo econômico.
§ 3º Se da invasão resultar a obtenção de conteúdo de comunicações eletrônicas privadas, segredos comerciais ou industriais, informações sigilosas, assim definidas em lei, ou o controle remoto não autorizado do dispositivo invadido:
Pena - reclusão, de 6 (seis) meses a 2 (dois) anos, e multa, se a conduta não constitui crime mais grave.
§ 4º Na hipótese do § 3o, aumenta-se a pena de um a dois terços se houver divulgação, comercialização ou transmissão a terceiro, a qualquer título, dos dados ou informações obtidas.
§ 5º Aumenta-se a pena de um terço à metade se o crime for praticado contra:
I - Presidente da República, governadores e prefeitos;
II - Presidente do Supremo Tribunal Federal;
III - Presidente da Câmara dos Deputados, do Senado Federal, de Assembleia Legislativa de Estado, da Câmara Legislativa do Distrito Federal ou de Câmara Municipal; ou
IV - Dirigente máximo da administração direta e indireta federal, estadual, municipal ou do Distrito Federal (BRASIL, 2012).

However, many computers, phones and smartphones do not have such security mechanisms, and often, even though they have, they are not connected. In any case, these "computing devices" will not be protected by this criminal law (BITENCOURT, 2013 apud SANCHES, 2015, p.246). Also, in this bias, when accessing a computer device that does not have a security mechanism, the subject who does it without circumventing the device, fails to complete the elementary of the criminal type *"through an improper breach of security mechanism"*. Therefore, this agent committed an atypical act for lack of the elemental incriminating alluded to, fundamental element of the criminal conduct. In this way, by complementing the criticism, Greco (2013) proposes that the term *"by improper breach of security mechanism" should*be replaced by *"without authorization"*. The author justifies this proposal by stating that, as it was drafted, it prevents the real criminal imputation, since "for the purposes of a typical configuration, in view of the requirement contained in the criminal type under analysis, there will only be a criminal offense, if any, by the invading agent , an improper breach of the security mechanism (GRECO, 2013, p.292).

Continuing the critical analysis of article 154-A of Law No. 12.737 / 2012, there are other questions about what is a "*computer device*" and "*security mechanism*". The first term encompasses a myriad of existing computing devices such as *computers, smartphones, notebooks, tablets, external HDDs*, among many others that will still emerge, with the ability to store data that can be tampered with. In the second expression, the legislator also opted for an expression that includes the various specific types of existing mechanisms as well as those that emerge. Therefore, any device or security mechanism that may be developed will be framed in the said Law. However, in some cases, the terms "*computing device*" and "mechanism *security*" are questioned due to the criteria used to distinguish them. As an example, one wonders if the blocked screen of a *Smartphone* could be considered a security mechanism, or if a watch could be considered a computer device. The Carolina Dieckmann Act makes no mention of such criteria.

In analyzing the aforementioned article 154-A, it is necessary to observe the elementary *"for the purpose of obtaining, adulterating or destroying data or information without express or tacit authorization"*. The new incriminating criminal type carries the subjective element of the type that consists in punishing malicious conduct when obtaining, adulterating or destroying data or information, that is, specific malice. However, thesubject*Hacker* enters the systems and computer devices of others only to test and show their abilities, that is, the subject has the purpose, simply, to demonstrate that such a vulnerable system. Therefore, it is perceived that the subjective element of the criminal type under analysis is the fraud, the free and conscious will of the agent to obtain, adulterate, or destroy data, being thus, hacker that only accesses the computer system or device, practice fact atypical, because it entered without the intention of obtaining, adulterating or destroying data. CAPEZ explains that the elementals come from element, which means fundamental basic component, thus configuring all the fundamental data for the occurrence of the typical fact, which, in its absence, the typical figure disappears (CAPEZ, 2012, page 381). The same author also conceptualizes elementary as "every essential component of the typical figure, without which it disappears (absolute atypicality) or becomes (relative atypicity)".

It is always in the so-called fundamental type or basic type, which is the caput of the incriminating type (CAPEZ, 2012, p.475). Thus, for the characterization of the criminal type provided in article 154-A of Law 12.737 / 2012, there will be a need for the conduct of the criminal agent to fill the elementary type, which according to Greco (2012) consists of invading a device improperly accessing, tampering with, or destroying data from the owner of the owner's device as well as to use such data to gain an unfair advantage. For Greco (2012), in the absence of one of these elements, will make the conduct atypical. Thus, Greco (2012) explains that even if the lack of some elementary of the incriminating criminal type, criminal conduct were considered typical, it could be concluded that connecting to a wireless network without a password, the neighbor, would be considered a fact typical.

(IN) Compliance with the principle of proportionality in the strict sense: Before entering into (in) compliance with the principle, this search within criminal law maintains a balance between the creation of new penal types with the penalties commenced. Capez (2007) explains that in cases of computer crimes, which have as their object goods not protected by the CPB, their conduct must be considered. It thus clarifies that the creation of criminal offenses and the imposition of penalties should be proportionate. The penalties imposed by the legislator should be applied in a moderate manner, weighting them with the seriousness of the criminal infraction committed by the individual with the objective of guaranteeing the fundamental rights brought by the Magna Carta, which according to Nucci (2011) should be applied according to with the seriousness of the criminal offense committed, that is, on a proportional basis.

Thus, Nucci (2011, p. 92) doctrine that the principle of proportionality is attentive to the penalties applied and their gravity, so the penalties must be proportional to the seriousness of the criminal infraction. In this sense, when Law 12.737 / 2012 is invoked to apply criminal sanctions, these should be made in proportion to the crimes committed through the Internet, not accepting exaggerations or misconceptions on the part of the legislator. As regards (non) compliance with the principle of proportionality in the strict sense, it should be pointed out that the legislator in drafting the standard did not comply with this principle. The activity of the legislator should always be regulated by a judgment of moderation between the gravity of the crime to be prevented and the sentence imposed, by offending the fundamental principles listed in the Federal Constitution. Brazilian criminal justice is against disproportionality. The principle of proportionality seeks to avoid exaggeration by depriving the legislator of exaggerated and unnecessary penalties. However, it is stressed that this principle also has the power to prevent punishment below the measure, ie the prohibition of insufficient criminal legal intervention. In this sense, Queiróz (2012, 80) teaches that "the principle of proportionality includes, in addition to the prohibition of excess, the prohibition of insufficient criminal legal intervention". So, it is with these teachings that the disproportionality introduced by the legislator is demonstrated by bringing, in the text of article 154-A, of the Brazilian penal code, punitive measures to the crime of invasion of computer device. In an analysis of the article quoted above, it can be concluded that the penalties brought are insignificant and insufficient in the protection of the legal right - privacy. The text of article 154-A criminalizes the conduct "to invade another computer device, connected or not connected to the

worldwide computer network, through an improper breach of security mechanism". The penalty imposed for this criminal type is detention, from 3 (three) months to 1 (one) year, and fine; and for the cases provided for in the *caput* of Article 154a and in paragraph 1, penalties shall be increased from one sixth to one third "if the invasion results in economic loss". That is what establishes Law 12.737 / 2012, art. 154-A[2]. It should be noted that this increase is applicable only to the figures described in the *caput* and the respective paragraph 1 of article 154a, prohibiting their applicability in qualified cases. In analyzing this article, it is verified that the legislator chose the sentence of detention, carried out in semi-open regime, for the execution of sentence of deprivation of freedom for those who commit computer crimes. A fact that prevents this regime from complying with the sentence is applied to all, since this decision falls to the magistrate, as affirmed by Nucci (2005).
That being so, it is clear that the penalty provided by the legislature is inadequate and ineffective, and in consideration of the principle of proportionality in the strict sense, which is aggregated with the function of general penalty prevention. For the insignificant amount of sentence imposed by the legislator will hardly intimidate internet offenders.

It may also be added that the maximum sentence imposed on computer crime even with the fine does not exceed two years, characterizing a criminal offense of less offensive potential judged by the Special Criminal Court of Law n. 9.099 / 95, with all the corresponding decriminalizing institutes. Therefore, the criminal, instead of being penalized with a custodial sentence, even in the mode of detention, will be favored with the criminal transaction and the conditional suspension of the process. In Bitencourt's (2013) conception, undoubtedly, the disclosure of intimate photos, for example, has to be punished in a more rigorous way when compared with a mere invasion. This is because it creates irreversible consequences for users who are victims, especially when the disclosure is made through the worldwide computer network. However, the normative text was not able to cover hypotheses as serious as those typified, which also needed a greater penalty, such as the dissemination of intimate photos obtained through computer devices, as previously explained. That being so, the criminal subject who commits the crime foreseen by article 154-A, of Law 12.737 / 2012, even though he has increased his sentence, will hardly be imprisoned. In this context, it is clear that when the legislator fails to correctly apply the principle of proportionality, at the moment of imposing the penalty in the abstract, the rule becomes unfair and inefficient.

Final Considerations: The number of undiscovered and unreported computer crimes in Brazil is high and, despite the controversies, the reluctance of those involved in reporting incidents or disclosing any information associated with computer crimes, such as companies insurance and banking institutions, because of the fear of losing the confidence of its shareholders, customers and investors with adverse publicity. Another factor to be observed is the lack of technical preparation by the police authorities, the difficulty of proving and detecting the practice of computer crimes, but the most neglected factor is the lack of adequate criminal legislation on computer crimes. The solution to the problem is not only to adapt extra-legal measures, such as electronic virus security measures, authenticity verification and security of sites in which electronic transactions will be carried out, among others, but also legal, such as adequate legislation and legal measures such as codes of conduct, with principles and behavioral modes for navigation, data traffic and virtual rights of users in the computer network.

Brazilian criminal law is still immature in relation to criminal offenses committed through the internet because it does not protect all legal assets threatened by virtual criminals. However, this immaturity of criminal law does not prevent the competent bodies from working to combat this new form of delinquency. In the specific case of Law 12.737 / 2012, through the analysis of the text of article 154-A, it was possible to verify flaws in the wording of the text, as well as gaps that prevent proportionality of the criminal type. In Article 154-A of the aforementioned Law, the practice of the crime of invasion of a computer device, considered a crime of less offensive potential, implies in the jurisdiction of the Special Criminal Court, as provided in Law n. 9999/1995, and it is the responsibility of the judge to determine how the sentence is to be served. Although it represents an advance in the absence of specific legislation to deal with cases of invasion of computer devices, Law 12,737 / 2012 did not solve the problem of criminalization of this type of conduct, and was ineffective.
It is hoped, therefore, that future draft laws on computer crimes will be elaborated in a more precise way, paying attention to the reality of information technology and the *internet*, otherwise, Brazil will continue in its current position: crime and lacking efficient laws.

REFERENCES

_____, Renato Opice. Crimes eletrônicos – a nova lei é suficiente? fev. 2013. Disponível em: <http://www.migalhas.com.br/dePeso/16,MI172711,101048-Crimes+eletronicos+a+no va+lei+e+suficiente> Acesso em: 10.mar.2019.

_____, Sônia Aguiar do Amaral. Inviolabilidade da Vida Privada e da Intimidade pelos Meios Eletrônicos. São Paulo: Editora Juarez de Oliveira, 2002.

_____, Tulio Lima; Fundamentos de direito penal informático: do acesso não autorizado a sistemas computacionais. Rio de Janeiro: Forense, 2003.

_____. Câmara dos Deputados. Resolução nº 17, de 1989. Aprova o Regimento Interno da Câmara dos Deputados. Diário do Congresso Nacional. set. 1989.

_____. Código Penal. Brasília, DF: Senado Federal, 1988. Disponível em: <http://www.planalto.gov.br/ccivil_03/decreto-lei/Del2848compilado.htm>. Acesso em: 12.mar.2019

_____. Lei nº 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>. Acesso em: 30.mar.2019.

[2]Art. 154-A. Invade another computer device connected or not to the computer network through improper breach of security mechanism and for the purpose of obtaining, tampering or destroying data or information without the explicit or tacit authorization of the device owner or installing vulnerabilities to gain an illicit advantage:
Penalty - detention, from 3 (three) months to 1 (one) year, and fine.
Paragraph 1 - In the same penalty, anyone who produces, offers, distributes, sells or distributes a computer device or program in order to allow the practice of the conduct defined in the caput.
Paragraph 2. The penalty is increased from one sixth to one third if the invasion results in economic loss. (BRAZIL, 2012).

_____. Lei nº 9099, de 26 de setembro de 1995. Dispõe sobre os Juizados Especiais Cíveis e Criminais e dá outras providências. Disponível em: <http://www.planalto.gov.br/ccivil_03/Leis/L9099.htm>. Acesso em: 25.mar.2019.

<http://www.gazetadopovo.com.br/vidapublica/justicadireito/artigos/conteudo.phtml?id=1362035&tit=A-nova-lei-de-cries-digitais> Acesso: em 11.mar.2019.

ALBUQUERQUE, Roberto Chacon de. A criminalidade informática. São Paulo: Juarez de Oliveira, 2006.

BASTOS, Celso Ribeiro; MARTINS, Ives Gandra. Comentários à Constituição do Brasil. vol. 2, São Paulo: Saraiva, 2001.

BATISTA, Emerson de Oliveira. Sistemas de informação: o uso consciente da tecnologia para o gerenciamento. São Paulo: Saraiva, 2006.

BITENCOURT, Cezar Roberto. Tratado de Direito Penal: parte especial, v.2– 17ª. ed. São Paulo: Saraiva 2017.

BLUM, Renato Opice. Crimes eletrônicos – a nova lei é suficiente? fev. 2013. Disponível em: <http://www.migalhas.com.br/dePeso/16,MI172711,101048-Crimes+eletronicos+a+no va+lei+e+suficiente> Acesso em: 12 novembro. 2017.

BRASIL. Constituição da República Federativa do Brasil. Brasília, DF: Senado Federal, 1988. Disponível em: <http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm>. Acesso em: 12.mar.2019.

CAPEZ, Fernando. Curso de Direito Penal – Parte geral. 11 ed. São Paulo: Saraiva 2007.

CASTELLS, Manuel. A Era da Informação: economia, sociedade e cultura, vol. 3, São Paulo: Paz e terra, 2006

CASTRO, Carla Rodrigues Araújo de. Crimes de informática e seus aspectos processuais. 2. ed. Rio de Janeiro: Lumen Juris, 2003.

CORRÊA, Gustavo Testa. Aspectos jurídicos da internet. São Paulo: Saraiva, 2000.

CUNHA, Rogério Sanches. Manual de Direito Penal: parte especial, 8ª edição. Salvador: JusPODVM, 2016.

DEL RE FILIPPO, Denise. Bem-vindo à Internet / Denise Del Re Filippo, Alexandre Sztajnberg. — Rio de Janeiro: Brasport, 1996.

GRECO, Rogério. Comentários sobre o crime de invasão de dispositivo informático − Art.154−A do Código Penal. Disponível em: <http://www.rogeriogreco.com.br/?p=2183>. Acesso em: 21.mar.2019.

GRECO, Rogério. Curso de direito penal. volume II: parte especial, artigo 121 a 154-B. 10. ed. rev. ampl.. e atual. Niterói: Impetus. 2013.

IBOPE/NIELSEN. Perfil dos usuários de sites de comércio eletrônico. Disponivel em: http://www.ibope.com.br. Postado em 2010. Acesso em 03.maio.2019.

KOTLER, Philip. Marketing para o século XXI: como criar, conquistar e dominar mercados. São Paulo: Futura, 1999.

LAUDON, Kenneth C.; LAUDON, Jane P. Sistemas de informação gerenciais. Tradução Thelma Guimarães. 7. ed. São Paulo: Prentice Hall, 2007.

LÉVY, Pierre. A inteligência Coletiva. Por uma antropologia do ciberespaço. Trad. Luiz Paulo Rouanet. São Paulo: Loyola, 1999.

NUCCI, Guilherme de Souza. Manual de Direito Penal - Parte Gerl. São Paulo: Editora Revistas dos Tribunais, 2013.

PINHEIRO, Patrícia Peck. HAIAKAL, Victor Auilo. A nova lei de crimes digitais. abril. 2013. Disponível em:

PRADO, Luiz Regis. Curso de Direito Penal Brasileiro, vol.2: parte especial, arts. 121 a 249. 11.ed. rev. Atual. E ampl. – São Paulo: Editora Revista dos Tribunais, 2013.

QUEIROZ, Alisson Araujo et al. A tendência da contabilidade diante das novas especialidades social, ambiental e tecnológico. Qualit@s Revista Eletrônica do Centro de Ciências Sociais Aplicadas, São Paulo: ano 2004

QUEIROZ, Paulo. Curso de direito penal – parte geral. v. 1. 8ª Edição. Salvador, Editora JusPODIVM. 2012.

REIS, Wanderlei José dos. Delitos Cibernéticos – Implantações da Lei 12737/12. Revista Jurídica Consulex, ano XVII, nº 415, 1º de dezemro de 2013. Disponível em: <http://www.tre-rs.gov.br/arquivos/REIS_delitos_ciberneticos.pdf>. Acesso em: 17.mar.2019

ROSA, Fabrízio. Crimes de Informática. 2. ed. Campinas: Bookseller, 2006.

ROSSINI, Augusto Eduardo de Souza. Informática, telemática e direito penal. São Paulo: Memória Jurídica, 2004.

SILVA, Cássia Lopes da. O direito penal e sistema informático. São Paulo: Revista dos Tribunais, 2003.

SILVA, Edson Ferreira da. Direito à Intimidade. São Paulo: Oliveira Mendes, 1998.

SYDOW, Spencer Toth, Crimes Informáticos e Suas Vítimas: 2ª.ed. São Paulo: Saraiva, 2015.

TANENBAUM, Andrews S. Redes de computadores. Tradução Vandenberg D. de Souza. 4. ed. Rio de Janeiro: Elsevier, 2003.

VIANNA, Tulio; MACHADO, Felipe. Crimes Informáticos. Belo Horizonte: Fórum, 2013.

VIEIRA, Fábia Magali Santos. Tecnologia da Informática aplicada na educação. Montes Claros: UNIMONTES, 2010.

****