ISSN: 2230-9926

Available online at http://www.journalijdr.com

IJDR

International Journal of Development Research
Vol. 11, Issue, 09, pp. 50541-50547, September, 2021
https://doi.org/10.37118/ijdr.22887.09.2021

RESEARCH ARTICLE OPEN ACCESS

CRIME IN THE DIGITAL ERA: A VICTIM-DOGMATIC ANALYSIS OF THE RISKS AT SOCIAL GLOBALIZED MEDIA

Paulo Sérgio Remígio Leão*[1], Ailma Cavalcanti Almeida[1], Reginaldo Inojosa Carneiro Campello[1], Adriana Conrado de Almeida[3], Aurélio Molina da Costa[3] and Rosana Anita da Silva Fonseca[4]

[1]Faculdade de Odontologia, Universidade de Pernambuco
[2]Faculdade de Enfermagem N. Sra das Graças, Universidade de Pernambuco
[3]Instituto de Ciências Biológicas, Universidade de Pernambuco
[4]Faculdade de Ciências Médicas, Universidade de Pernambuco

ARTICLE INFO

Article History:
Received 11th August, 2021
Received in revised form
13th August, 2021
Accepted 01st September, 2021
Published online 30th September, 2021

Key Words:
Cybercrime, Internet Civil Mark Law, Cyber victim.

***Corresponding author:**
Paulo Sérgio Remígio Leão

ABSTRACT

Computer technology has come to stay in people's life and the coexistence between user and electronic computer devices would be harmonious if it were not for the undesirable action of malicious people, cyber criminals, whose activities may cause irreparable harm to their victims. This work now presented has as its main aim to highlight aspects inherent to the virtual environment from a victim-dogmatic perspective. It is a qualitative study, by using the descriptive and deductive method, which seeks to present the problem, by considering the reality of cybercrime and Brazilian legislation, the most effective Brazilian laws as Internet Civil Mark Law, the General Data Protection Law and, more recently, Law number 14.155/2021. The latter has allowed the competent authorities involved in the investigation and criminal procedure to access and exchange computer data of the investigated people and established more several penalties for criminals. Many cybercrimes are of a cross-border /transnational nature and, unfortunately, international laws are not the same at fighting against this kind of crimes. It is hoped that this article is able to provoke an important reflection on cybercrime in Brazil that can contribute to the establishment of more effective ways to fight it.

Citation: ***Paulo Sérgio Remígio Leão, Ailma Cavalcanti Almeida, Reginaldo Inojosa Carneiro Campello et al.*** "Crime in the digital era: a victim-dogmatic analysis of the risks at social globalized media*", International Journal of Development Research*, 11, (09), 50541-50547.

INTRODUCTION

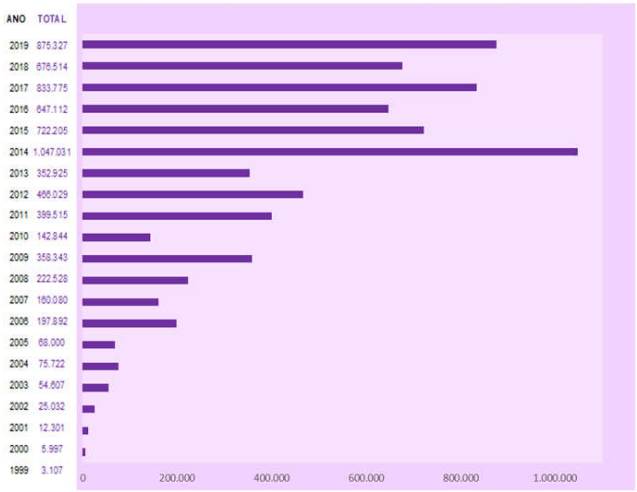
Nowadays, our world is experiencing the so-called "Digital Revolution" and the "Information Society", by using the world net of computers, the INTERNET, as an agent for modifying the behavior of users who, anxious for speed and technology, move simultaneously in the physical and digital environments (Rossini, 2009). The impact caused by Internet on human society has brought educational, economic and political changes all over the world, especially at this time of the pandemic called Covid-19. Besides educational portals, e-commerce sites and job search, web browsers make it easy to access cybercrimes (Urrahman *et al.*, 2020). Cybercrime is a result of security weakness for world wide web users and, in particular, those frequent users of social networking sites.

In this sense, the more users of this kind of social communication the more possibilities of comittingcybercrimes. According to annual report of Cyber Security (2019) cybercrime is on the rise and forecasts an expenditure of 6 trillion dollars in 2021 (3 trillion dollars in 20115). Due to its profitable nature and low risk for the aggressor (since cybercriminals can launch attacks from any place in the world, cybercrime tends to perpetuate itself (URRAHMAN *et al.*, 2020). According to Lallie*et al.* (2021), computer and data security requires the urgent creation of its own legislation with adequate punishment mechanisms. The protection of human rights in this kind of crime constitutes an extremely important mechanism to provide society security, otherwise it is going to open space for a series of injustices which vary according to reasoning line of each magistrate who, in most cases, is unware of the cybernetic universe and its peculiarities. Taking into account the number of people, many of these lives are

taken prematurely, quite before the judgement of the merits, when the cases are judicialized, or even in the initial phase of the police investigation because of technical fragility in the operational scope of the expert body and other specialists, reason why crucial and urgent measures are needed for justice sake. More recently, Law nº 14.155/2021 of May 27, 2021, came into force to make several important changes in the conduct of investigating and prosecuting authorities for digital processes. This Law has established in its § 4th-B, an increase in the time of the theft penalty for cyber criminals that is now from 4 (four) to 8 (eight) years and a fine is expected, if the theft is committed through an electronic or computer device which, in turn, is or is not connected to Internet. This legal forecast is more comprehensive when the § 4th-B states that the crime may occur even without the violation of the security mechanism, that is, without the use of Malware, or any other equivalent fraudulent means. The penalty may also be increased, according to the harm resulting from the crime caused to the victim, if such crime incurs in an elderly person and if it is caused with the employment of foreign public servant. The penalty still increases from one-third to two-thirds in each case. This study presents a systemic approach to the entities involved in virtual criminal acts, observing the dogmatic victim perspective. The systemic approach refers to that set of theoretical currents which interpret the vitimological aspects, lit by the legal principles of the Democratic State of Law.

Information age - A historical retrospective: In the preamble of Federal Constitution of Brazil, in 1988, occurs the edification of a Democratic State, with a fulcrum in ensuring the exercise of social and individual rights of people. This Constitution is named Citizen Constitution, since it established freedom, security, welfare, development, equality, and justice as its supreme values of a fraternal, pluralistic and unprejudiced society, based on social harmony. Immediately one can perceive the birth of a free, fair and solidary society, protected by the action of the State (BRASIL, 1988). Computing or Data Processing made a revolution in people's lives and with it, computer Science. This last one standardized computer language and allowed simultaneous communication among people, enterprises and trade (STRUPCZEWSKI, 2021). The*Internet* has become the main component of a country's infrastructure and the primary foundation of social and economic activities all over the world. It spread quickly from the U.S. to Europe and Asia. The United States, where it was invented, is the leader in the Internet Development Index and in applications, industry development and governance (OLIVEIRA *et al.*, 2021). In 1999 social networks started emerging, each one of them with a different purpose, such as media sharing or microblog, serving as a question and answer forum. The contents are also different. S*hort Message Service* (SMS), *Orkut, Facebook, Instagram*, and direct connect apps like *Viber*, *WhatsApp e Telegram.* The revolutionary characteristic of *WhatsApp* was to replace for free, the *SMS*, charged by telefone operators, (BHATTACHARYA *et al.*2020). The constant technological advances and the expansion of its use has created the "information society" and, with it, cybercrime. (MEDEIROS, BYGRAVE, 2015).

Vulnerability at virtual environment: Violence is defined by World Health Organization (WHO) as the use of physical strength or power, in threat or practice against oneself or someone or a group of people or community which results or may result in suffering, death, psychological damage, impaired development or deprivation (WHO, 2002). Violence is the result of complex interaction of individual factors, family relationship, social, cultural and environmental. Realizing as these factors are related to violence is one of the most important steps at boarding public health for violence prevention. (DAHLBERG *et al*., 2007) In the virtual scope internet users become victims easily for the practice of cybercrimes when they make downloads of malicious apps and sites, which abuse the obligation to accept the legal terms, necessary for the installation of these cybernetic programs. Besides victims' fragility, cyber criminals are still favored, additionally, by the anonymity of the virtual environment, harming such victims in several degrees of intensity. (GALI *etal.*, 2021). Modern cities are increasingly endowed with information and communication technologies, including digital cameras, sensors and Wi-Fi tracking. These monitoring practices based on ICT data, however, change cities and their residents into extraordinary data capture apparatus, interfering with people's interests, preferences, emotional status and behavior, at much greater levels of scrutiny and control, as people increase their use of devices connected to the World Wide Web (GALI *etal.*, 2021). An important effect of the Covid-19 pandemic is straightly related to the workforce – people involved or available to work. The employees' mass quarantine, the adopted measures to exercise remote work, the fragility of cyber infrastructure at worker's homes, has created an environment propitious to cyberattacks (HARJINDER *et al.*, 2021). In addition to the enlargement of the users' screen in relation to the remote work, loneliness is added, caused by social isolation, adopted at facing the pandemic. There is, this way an increase in action opportunity for cyber criminals. As for loneliness, an alone individual who sails in search of pleasure and to be accepted in a society through *internet,* and find a half single way to stay long, will suffer cyberattacks (FIORILLO, 2016). The Center for Studies, Response and Treatment of Security Incidents in Brazil is an incident handling group with national responsibility that operates in all networks that they possess or Autonomous Systems allocated to Brazil or have domains registered under ccTLD.bror country code level domain (HOEPERS, 2020). Incidents recorded in recent years by this center are shown in Figure 1, which reveals an upward trend as years pass by. Multiple factors contribute to that trend, due to larger and larger number of users, attracting more and more interest of the criminals because of the great vulnerability. The great number of incidents in 2014 was due to three categories of attack: fraud attempts, scans, and denial of services. The notifications of fraud attempt this year, totalized 467.621 cases, number five times larger than the one in 2013.



(Fonte: CERT.br)

Figure 1. Total de incidentesreportadosao CERT.br porano

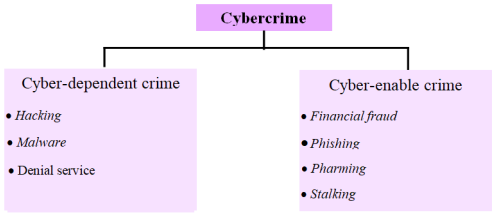


Figure 2. Cyber-dependentand cyber-enabled crimes CPS (2019) (adaptado de Lallie *et al*., 2021)

Please, put the Figure 1 here: Nowadays, because of technological advances (computers, mobile phones and the *Internet)* access to any information has become instantaneous. "One has the world in one's hands"texts and images sail among users of the "WWW" at an unimaginable speed before, motivated for distinct interests, good or bad ones. In delituous pornographic aspect, the cyber attacker adopts so extreme an action that he may provoke irreparable damages in his victimsIt is urgent that these dangerous criminals, conduct be fought

by the authorities in accordance to the law, for punishing them effectively. The attacks may be classified as active and passive. In the first case the invader tries to alter the system resources or affect their functioning, while, in the second case, the invader tries to learn or make use of data obtained in in the program, but he is not able to affect their functions. In passive cyberattack, the invader uses a secret behavior that can represent, for instance, a sequence of operations that he cannot know or the reach of a specific state in which the system is more vulnerable to an active attack (Lima et al., 2020). Similarly, an individual expose himself in two ways: active and passive. In the active way, the user has no worries about his cyber safety and his reckless browser puts him at imminent risk. In passive exposure, the user navigates by using reliable and secure technological platforms. In digital world, users provide their data to third parties on numerous websites and internet applications, without any safety in relation to misuse, what may take to data leakage and to cybercrime, causing harm to natural and legal persons and to the state itself (PEREIRA *et al.*, 2020).

Risk society or society that takes risks in the virtual age?: It is public and perfectly known that the virtual society is composed by people, identified through a *TCP/IP* protocol joined to an operational platform of hardware (machines) and software (programs), able to provide instantly communication and interaction. In this aspect the *Internet* is, in theory, an ideal society. The computer society, however, coexists along with a continuous exposure to the action of a class of people who take profit from *internet* users' fragility, by committing cybercrimes. The speed in the interlocution between people and commerce would be healthy, with the greater permanence in the search for relationships, if there were no cybercrimes. (REILLY, 2021). Internet users' fragility before criminal's threat in digital spaces is mitigated by privacy models to avoid damage caused by violations. In fact, corporate interests who take advantage from continuous digital surveillance on line, purposely obscure their activities, thus complicating users' ability. Although some protection behavioral individually started by more informed users may be efficient in reducing localized damages, legal and significant reforms are needed for lasting protection of all users (REISACH, 2021). The usage of new technology for communication presents risks. If on one hand there is a user's lacking information, on the other hand may exist another malicious user who takes advantage of false anonymity and a mistaken notion of impunity, due to the difficulty of tracking the author and almost impossibility of applying the legislation in force. Encryption and digital signature are some auxiliary mechanisms in the protection of internet users' legal assets. So the risky society is that one which is fragile before malicious actions by cyber criminals (MARRA, 2019). Common virtual crime is that one that uses internet only as the means to carry out the crime already typified by penal law. (MALAQUIAS, 2015). Such as traditional crime, three factors have to be present in the cybercrime: one victim, one reason, one opportunity. The victim is the attack target, the reason is the aspect that drives the criminal to commit the attack and the opportunity is a chance for the crime to be committed (LALLIE, 2021).

Crown Prosecution Service (CPS) from United Kingdom classifies cybercrimes into dependent and independent ones. (CPS, 2019). A cyber dependent crime is that one which can only be committed by using a computer, a computer network or another form of information communication technology. Independent cybercrimes are traditional ones that can be increased in scale or reach by using a computer, a computer network or another form of information communication technology. Those categories, as well as examples of their subcategories, can be seen in Figure 1. Some of the described elements are often interconnected in a cyber-attack. For example, an e-mail of phishingor text message (SMS, WhatsApp) can be used to attack the victim for a fraudulent website. Then the site may gather personal data that can be used to commit financial fraud or install malware (ransomware, more specifically) which is used to commit extortion.

Please, put the Figure 2 here: Dependent cybercrimes are those ones which invade the computer and provokes interruption or degradation of the computer function, as hacking, malware and denial of service Hacking is a kind of invasion directed to computers, mobile phones and personal tablets. Malware (malicious software) is a disturbance of the computer's functionality. It spreads among computers and can be destructive, for instance, at excluding files or causing failures in the system, but it can be also used to steal personal data. The types of malware include virus, worms, Trojans, spyware, ransomware. Viruses require a host (like a file) in a computer to act as a porter. Worms are self-replicating programs, but they can spread autonomously, into and among computers, without requiring a host or any human action. They can also be used to insert Trojans on the network system. Trojans are programs that introduce themselves as useful, routine and interesting to persuade the victim to install them. This malware can perform functions such as stealing data without the user's knowledge and can trick the user into doing a routine task while performing a hidden and unauthorized action. *Spyware* is a *software* that invades the user1s privacy, gathers confidential information and monitors visited websites. These data can be transmitted to third parties. Sometimes, the spyware can be hidden in the adware (free software and, sometimes unwanted, that requires your attention to ads at using them) An example of spyware is that one which captures the sound of computer keystrokes and reveals sensitive data such as passwords or details of bank accounts. *Ransomware* is a software that can keep your data as hostages, for instance, a Trojan can copy the contents of the "My documents" folder into a password-protected file and delete the original one. Then the cybercriminal will be able to send a message requiring a payment in exchange for accessing the folder.

The malware can be spread by spam, unsolicited e-mail or not targeted junk (CPS, 2019). Independent cybercrimes are those ones that do not depend on computers or networks, but have been changed into scale or shape through internet and communication technologies. They are part of the following categories: cybercrime related to economy and this type of crime includes: fraud, intellectual property crime (piracy, counterfeiting), malicious and offensive communications, including *cyberbullying*, cyber violence against women and girls, through the dissemination of sexual images, cyber harassment, child sexual offenses, child sexual abuse, enticing children to obtain indecent images, pornography, obscene publications and prohibited images. Phishing scams are a specific type of mass marketing: they specifically refer to the use of fraudulent e-mails disguised into legitimate ones that solicited or fish users 'personal or corporate data, for example, passwords or bank account details. Phishing mass attempts may be sent to a variety of potential targets. Pharming occurs when a user is directed to a fake website, sometimes through phishing e-mails to insert his personal data and frauds of romance on line (or social network/dating site) Individuals can be contacted through social networks or dating sites and persuaded to furnish personal data or money after a long online relationship (CPS, 2019). Changes in work practices and socialization mean that people spend more time online. The combination of growing levels of attacks and cybercrimes implies an increase in constant surveillance not only by the user but also by government authorities to curb this type of crime all over the world. Law enforcement must ensure these authorities, ability to deal with cybercrime. In cybercrime investigation, law enforcement agencies follow techniques similar to that used in traditional crimes, which, however, need to be modified to meet the unique conditions and requirements of the virtual space (BUTKOVIC *et al.*, 2019).

Victimology and victimdogmatic: awakening to legal awareness: Cyber criminology is a branch of criminology that studies the personality of cybercrimes victims. Criminology has showed that, in many cases, the simple general prevention has not been enough to prevent the action of the cybercriminal. This statement is consistent when the victim realizes that his behavior in virtual environment is encouraging for delituous action. (SYDOW, 2015). Studying the victim and his conduct or unconscious contribution for the crime occurrence is verifying critical criminology, that also proposes

efficient solutions of prevention through models of concrete technics of intervention in the action of the delinquent individual. (ARRUBLA, 1986). Criminal behavior must necessarily involve a perpetrator and a victim. Despite the obvious need for this relationship, the criminal has always received the largest part of public attention, the legal system and academic research, in order to understand the circumstances, motivations and behavioral factors that take to the perpetration of a criminal action. On the other hand, the victims have been, in great part, the group whose focus is the care and welfare in relation to the crime. This attention bias tends to the provision of a more balanced exploration of the two sides of the criminal act. On the victim dogmatic perspective, the victim figure is no longer a mere spectator and becomes the main object of the study, together with the perpetrator of the criminal act. In this typification, cybercrime is very similar to formal material crime. Several models have been proposed to help explain aggressors' and victims' characteristics and the form as these characteristics influence the risk of offending and/or of becoming victim of a criminal act (BROTTO *et al.*, 2017). The analysis under the victim dogmatic perspective fits as a central question about unconscious participation of the victim, as, for instance, to what extent the victim is passive or active subject of the process, when protected by anonymity? (MARRA, 2019). It is noteworthy that when the user accesses an unprotected computing device and displays a list of confidential customer information, one cannot classify as criminal conduct of theft when there is no intention, appropriation to his device or disclosure of information from his own computer (SYDOW, 2015).

Computer Crimes: a reflexive approach in Brazil: Brazil adopts the tort legal reserve system, that is, there is no crime if there is no law that defines it, and Brazilian legislation took a long time to recognize the techniques and behaviors of information technology. Sydow (2015) typified cybercrimes as follows: appropriate and inappropriate computer crimes. Appropriate ones are those in which the affected legal assets lack legislative regulations, because the target of the violation are computer devices, including data, programs and computer systems. Inappropriate offenses are the crimes committed by using the computer tool as a spontaneous way of choice by the offender, but it does not suggest new criminal legal concepts. It has to be emphasized that appropriate crimes, those which the target is computer technology itself deserve special attention, because criminal legislation in Brazil has gaps which must be adequately filled by facing the principle of legal reserve. In inappropriate crimes, computer technology is only the means used for the violation of legal assets – are already provided for in Brazilian penal code (JESUS, 2016) and the general characteristics of which make reference to conduct, action, omission and not fundamentally to the way the conduct was performed (TEIXEIRA, 2018). Some delituous or criminal conducts provided by Brazilian Penal Code may also be committed through Internet. Bank frauds, datatheft, confidential information, crimes against honor, racism, e-mail violation, copyright infringement , child pornography, software piracy, illegitimate interception, data interference, interference in systems, use of someone else's device without proper permission, falsehood or computer fraud, computer graffiti, defacement (altering the layout of web pages, sites, intranets, sending of unwanted messages, among others that we use the world wide web only as a way of their execution (TEIXEIRA, 2018). Although appropriate crimes are provided in Brazilian legislation, those crimes committed through computer devices are not yet properly provided in law and, therefore, they need effective normative that brings legal certainty to users and owners of these computer devices.

Brazilian legislative frameworks: some fundamental consideration

Law nº 12.735/2012 – Azeredo Law: The Law under discussion aimed to typify the conducts carried out through the use of a computerized system. This Law altered the Decree-Law nº 2.848, of December 7, 1940- Penal Code, the Decree-Law nº 1.001, of October 21, 1969 – Military Penal Code, and the Law nº 7.716, of January 5, 1989. This Law introduced delituous conducts performed from the use of electronic system, digital or similar, against computerized systems, but did not add any new penal type to the current legal system. (JESUS, 2016), nor predicted computer crimes practice against the common citizen. In this Law, legislators wasted the opportunity to insert some innovative computer crimes, already typified in the world, namely: unauthorized access, alteration and/or improper obtaining of data, password hijacking, malware production (SYDOW, 2015). Due to the lack of legal provision for the occurrence of cybercrimes, it is believed that a large part of these offenses will end up being tried at the federal level, given the cross-border and transnational nature of crimes, although the state level also has its responsibility in this judgement. Each Federal State, in Brazil, has the responsibility of making efforts to empower, train and specialize its investigative police, adequately increasing the number and capacity of its competent judicial experts and making them focuses on virtual and electronic investigation, in order to support judicial decisions for the exact application of the penalty.

Law nº 12.737/2012 – Law Carolina Dieckmann: This normative act had its origin in the historic episode of the leak of intimate photos of the actress, during the technical maintenance of her computer. These photos were illegally obtained, with a crime of extortion occurring, due to unauthorized access to the victim's personal data. This law typifies the crime of invasion of computer device and brings interesting legislative changes, by considering the most recent penal types. Many scholars understand such level of crime, that personal data must be respected for being relevant and that has to exist protection from the criminal legal system, but this understanding is not unanimous yet. By considering the institutional effort in the federal and state spheres in Brazil, this problem is quite far from being solved, as the punishment referred at this law does not consider this case an illegal and not authorized one (JESUS, 2016). If someone, for instance, accesses an open, vulnerable computer and finds a page whose content is confidential and obtains some illegal advantage from this, such gesture is not considered a crime, because there was no any previous intention to install vulnerabilities. (SYDOW, 2015).

In this area, weighing the issues related to access, it is still necessary to consider the fragility of the legislation as for the competent user to grant authorization, if a minor, or one with mental difficulties, or a lay person in technology, or in another language – which makes it very difficult the understanding of procedures related to software. The authorizations, therefore, could be directed to the addiction of consenting, due to error, fraud or even coercion. The solution for the problems arising from the several criminal modalities is difficult to be found in short time. Questions from that level are not solved only with edition of new laws, but, above all, with efficient public and criminal politics, continuous digital education and a robust investigative framework. All these actions are important measures to combat cybercrimes in an effective way.

Law nº 12.965/2014 - Internet Civil Mark: Law Project nº2.126 joined the National Congress in August 2011, posteriorly to the phase of popular participation, with the aim of establishing principles, warranties, rights and duties for the users of the world wide web, reason why, after being sanctioned by the Presidency of the Republic on April 23, 2014, becoming Law nº 12.965, it became known as "Internet Civil Mark". This Law had as its basic principle, to avoid contradictory decisions and legal uncertainty in questions related to digital crimes (JESUS, 2016). Laws nº 12.735/2012 and nº 12.737/2012 addressed in the items that preceded this one, focused on typifying some cybernetic facts and predicted the importance of the judicial police bodies, in the administrative procedural stages, regarding the structuring of regulations, sectors and teams specialized in combating digital crimes. The *Internet Civil Mark*, therefore, structured the obligation of internet providers or computer services to register logs of users' activities. The connection to the regardless of users' intentions, is only possible through an ISP(Internet Service Provider), to access *Internet,* which attributes to the users an address, known as IP (InternetProtocol) able to keep relevant information about the user's access to that device as follows: date, time,

connection permanence, access types, among other ones. This Law also obliges the Internet provider to identify and register the events that occur in a computer system to a person through IP and ISP, respectively. However, the obligation of furnishing these registers, to subside investigative phases of judiciary police is only possible through a court order. It is important to highlight that these measures are unavoidable to clarify the tort, but such complex requirements reduce the speed of court decisions in some years, sometimes, maximizing the risk of impunity. The *Internet Civil Mark* has not yet reached maturity and there are controversies within society about its effectiveness.However, there is no doubt that it is a necessary normative record that establishes an important legislative policy for taking in account the urgency and detailing of the desired legal security items for the common citizen in digital age.

Law nº 13.772/2018: This Law recognizes that violation of a woman's intimacy constitutes domestic and family violence and criminalizes the unauthorized registration of content with nude scenes or sexual or libidinous acts of an intimate or private nature. This Law altered the Law Maria da Penha and the penal code, making it possible to recognize that the unauthorized exposition of sexual intimacy, article 216- B of Brazilian Penal Code, provides for imprisonment from six months to one year and a fine. It is also applied to those who perform photo, video or audio montage with the aim of including a person in their intimacy. In this way, this legislation reveals a concern with women, victims of violence, not only in the physical environment, but also in the virtual one.

Law nº 13.709/2018 – General Personal Data Protection Law: Law nº 13.709/2018, December 19, 2018, is an important legislative mark which came into force in September 2020, has come to regulate the usage, protection and transfer of personal data in Brazil, ensuring control over Brazilian citizens, about their personal information. Known as the Individual Protection Law, it requires the explicit consent of users for the collection and use of their data and requires the offer of options, so that the Internet users can view, correct, confirm or delete these data. The scope of this Law had immediate repercussion on the care of cybersecurity in government administrations, the Union, States, Federal District and Municipalities. This Law presents important fundamentals as privacy respect, informative self-determination, freedom of expression, information, communication and opinion, inviolability of intimacy, honor and image, economic technological and innovation development, consumer protection, human rights, free personality development, free initiative and competition, dignity and citizenship exercise by natural people. This Law contemplates any treatment operation performed by natural or legal person of public or private law regardless the means, the country or where the data are located, as long as it is in national territory. It is important to highlight that the data treatment activity covers the offer, supply of goods and services, including by Brazilians or foreigners present in Brazil, during the cyber invasion. The Law does not cover, for the purposes of processing personal data, those ones carried out by a natural person for exclusively private and non-economic, journalistic, artistic and academic purposes, applying to this hypothesis the seventh and eleventh articles of the said law. Furthermore, the Data Protection Law goes far beyond the national territory. This restrains data on public security, investigation activities and prosecution of criminal offenses for the exclusive purposes of competent national and foreign government bodies, since the country of origin provides a level of personal data protection adequate to that provided for in this law.

Bill of Law nº 4442/2019: The Bill of Law presented in August 13, 2019, authored by federal deputy Felipe Carreras - PSB/PE and proposed by Delegate Eronides Menezes, from the Police Office for Repression of Cyber Crime in Pernambuco, aims to amend Law 12.965/2014 (*Internet Civil Mark*). The proposed alterations are very significant. The following ones are highlighted Article 10, 1st §, comes into force, expanding the competence for the police authority to request data from access providers, who hold information that can contribute to the identification of the user, or the computer device that contains the data (computers domestics or not), *notebooks*, *smartphones, tablets*, *mobile phones*, *pen drive, ad,* among similar ones). This alteration has important reflex in the celerity in the investigative process, considering the peculiarities and difficulties inherent to the physical environment. At 3rd §, the caput provisions do not prevent direct access to registration data, in accordance to the law by administrative authorities that have legal competence for the request, even in the investigative phase. The article 13 determines that it is up to the administrator of the autonomous system of internet connection provision, the obligation of keeping the connection registers under secrecy, control and protection for two years (it was only six months, before) This time dilation of information detention by the provider allows the specialized police a larger time to investigate cybercrimes, which are of a very complex nature. Among other important proposals at Article 18. 1st §, with the aim of combating hostage, access and availabilityof illegal content, even abroad, the delegate is allowed to request the unavailability or blocking of access to the aforementioned service from connection providers, within a period of up to 48 hours, regardless of a court order. Besides, 2nd § emphasizes that the request has to be clear and specific, with regard to the content identified as fraudulent or infringing and 3rd§ warns that non-compliance will result in civil and criminal liability. The proposal of legislative alteration is not only necessary but urgent, because the choice of a digital environment, for crime commitment, in general way, became too attractive to the criminal who cunningly knows the system fragility and the consequent juridical insecurity of internet victims.

***Law*nº 14.155/2021:** This Law came into force from May 28, 2021. Its text alters the Penal Code (Decree-Law 2.848, de 1940) to aggravate penalties for crimes such as device invasion, aggravated theft and embezzlement occurred in digital media, connected to internet or not. According to this Law, crime of computer device invasion is applicable to that individual who invades a device in order to obtain, adulterate or destroy data or information, without the owner authorization, or still install vulnerabilities to obtain illicit advantage. This Law also establishes punishment with reclusion, from one to four years and fine, getting larger the penalty from one to two thirds, if the invasion results in economic loss. In reclusion penalty, the compliance regime must be closed. The detention, which is applied to lighter convictions, the beginning of its compliance is not, necessarily, in a closed regime. But if the invasion provokes obtainment of content from private electronic communications, commercial or industrial secrets, classified information or remote control not authorized of the invaded device, the reclusion penalty will be from two to five years and fine. This penalty was from six months to two years and a fine, before the sanction of this new law (BRASIL, 2021). Protecting the cyber space requires constant care of the competent authorities. Besides, it is necessary leadership attentive over technological novelties to manage the continuous political, educational, legal and international changes. For this goal, it is basic that information security covers cyber defense, physical security and protection of organizational data to reach fundamental principles such as confidentiality, integrity, availability and authenticity of such data. Furthermore, Lei nº14.155/2021, besides aims to fulfil relevant gaps in the normative structure of the nation in relation to cyber safety, has intention to establish measures that bring changes in the way as the institutions and individuals position themselves on such an emblematic theme to develop a cybersecurity culture through awareness and continuous training.

The importance of computer forensics for justice: The new crime model through computer technology is more and more advanced as time passes by. Personal data and behavior habits are constantly exposed in computer media. This huge set of information is automatically treated through sophisticated machines which use personal electronic devices in the hands of most people in the world (SYDOW, 2015). Nonetheless the little knowledge of computational tools of the largest number of users, common citizens, aggravated by the insufficient experience of professionals in this area, requires special attention for capacitation of experts in this field of knowledge, so essential nowadays. The importance of cyber safety is growing. Companies from different segments know well how challenging has

been to keep their secrets confidential and secure. Events like fraud, invasion by hackers and crackers, damage to computer networks, dissemination of viruses, and hijacking of data and confidential information, theft and illicit advantages terrify global companies, causing them huge financial losses (MARQUES *et al,* 2015). Forensic investigation is too costly and requires adequate structure, constantly updated. These measures take long to happen in countries with limited financial resources. To minimize such problems, it is too important the specialization of their investigative police and qualified professionals and toughen up their technological structure to reduce the criminal problem that is spreading frighteningly. The importance of the interaction of legal Science with other fields of human knowledge is imperative. The most probable consequence of this conduct is the establishment of justice and more social balance in court decisions. Computer forensics expertise is an essential requirement (FRANÇA, 2008). The phenomenon of cybercrime is a global and a growing one. Thus, urgent, constant and permanent surveillance against this new cyber weapon. If, on one hand, the population of computer devices users has increased with remote activities, on the other hand, the same population is exposed to the action of cyber criminals. Then cybercrime occurs At this moment the computational forensic presents itself as an action of potent relevance in its application. It is undisputed that the interconnected world broadens alternative paths for the practice of illicit activities that urgently require the improvement of penal effectiveness.

CONCLUSION

It is incontestable that Computing brought to humanity uncountable benefits in the most varied areas of Science. However, access to information through computing requires from the users' society a different looking, principally by considering that the World Wide Web is an environment that deserves caution for the utilization of the available technologies. The sensation of safety and untouchability transmitted, aggravated by the necessity of socialization, by the desire of relationship and growing confidence deposited in someone recently found in the virtual environment, maximizes the users' risk chances of becoming victims of cybercrimes. The victims' profile obeys a logical of emotional lack that is supplied by the premeditated attention of the cybercriminal who believes in his virtual anonymity. The *cyber*criminal believes that his delituous practice in the middle of the virtual environment will difficultly be detected and, this way, he finds in this environment a vast barn of opportunities for his criminal action. The cybercriminal knows that the prevention methods of cybercrimes are still inefficient, especially by considering that speed *on time* of propagation of new criminal modalities is greater than the arrival of knowledge by computer expertise and law operators. Furthermore, a large part of cybercrimes is of cross-border or transnational nature and international legislation is not unison on the typification of a cybercrime. It must be added that the absence of technical cooperation among nations increases these difficulties. Furthermore, Brazil, despite current laws and bills to enter in force, needs to invest heavily in legislative policies which respect the urgent necessity to regulate computer law, by preserving individual and collective guarantees preconized by the Citizen Constitution.

In despite of several kinds of violence in physical environment, the violence committed in the virtual environment is a controversial and highly complex topic for elucidation by the lack of studies and research in academic and legal circles, aggravated by people's difficulty and shame in exposing their intimacy and privacy, generating scarcity of testimonies from victims, due to fear, guilt and shame for perceiving themselves impaired in their sexuality and self-confidence. It's already more than time to expand these debates, by considering the plural society in which all of us, invariably, are inserted, because, regardless of being the matter so comprehensive, it must also be analyzed under the criminology bias, seeking to realize in other knowledge areas, the fundamentals of this human behavior that expands into the social core. People should be educated about the way organizations collect data in online environments, individually, but they do not possess the power to combat that surveillance. Some models of privacy are added to this imbalance of power inherent to the virtual environment, because they are propagated by corporate and government interests that combine privacy and confidentially and put the blame on the user, for having not taken measures to protect themselves against threats many times invisible and unforeseen. The true purpose of the self-management model is to convince users that their privacy is a kind of merchandise that they can and should negotiate, like access to content online. This false market view of privacy distracts users from robust ethical models of privacy as a human right and obscures the ubiquitous power differential online that puts ill-informed and disempowered individuals against powerful and technological sophisticated corporations. The troubling fact of this discussion suggests an urgent change on public entities' conduct involved in confronting virtual violence, since the investigative phase of the misdemeanor up to its judicialization. On this specific aspect, the creation of judicial unities specialized in cybercrimes all over the federation would be an excellent action for confronting cybercrimes that, for the plurality and complexity of the cases, requires a specialized team in Digital and Informatics Law. This study proposes continuous debates in academic, legislative and judicial environments, so that our society really knows deeply the imminent risk of becoming victims of these delituous beings.

REFERENCES

Arrubla, C. M. M. 1986. El consentimiento del sujetopasivo: de la infracción a la ley penal.*RevistaFaculdad de Derecho y CienciasPolíticas*, 75, pp. 11-37.

Bhattacharya, S *et al*. 2020. ImpactofstructuralPropertieson network structure for online. *Procedia Computer Science*, 167, pp. 1200–1209.

Butkovic, A *et al.*2019. Geographic profiling for serial cybercrime investigation. *Digital Investigation* 28, pp. 176-182.

BRASIL. Constitution1988.Enacted on October5th. Available<http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm>. Access on: August 23, 2021.

BRASIL. Lei nº 12.965/2014, onApril 23, 2014. Available <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>. Access on: August 23,2021.

BRASIL. Lei nº 13.709/2018, onAugust 14, 2018. Available<http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm>. Access onAugust 23. 2021.

BRASIL. Lei nº 14.155/2021, May 23, 2021. Available <http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/lei/L14155.htm>. Access on: August 23, 2021.

BRASIL. Decreto-Lei nº 2.848, December 7, 1940. Available<http://www.planalto.gov.br/ccivil_03/decreto-lei/del2848.htm>Access on: August 23, 2021.

BRASIL. Decreto-Lei nº 3.689, onOctober 3, 1941. Available inDecreto-Lei nº 2.848. Access onAugust 23, 2021.

BRASIL. Lei nº 12.735/2012, on November30,2012. Available in<http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12735.htm>. Access in: August 23,2021.

BRASIL. Lei nº 12.737/2012, November 30, 2012. <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13772.htm>. Access in: August 23, 2021.

BRASIL. Lei nº 13.772/2018, December 1, 2018. Available <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm>.Access onAugust 23, 2021.

BRASIL. PL 4442/2019, situation: appended to PL 808/2018. Available in <https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2214922>. Access onAugust 23, 2021.

BRASIL. Lei nº 14.155/2021, May 28, 2021. Available <http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/lei/L14155.htm>. Access onAugust 23, 2021.

BRASIL. Agência do Senado Federal. Available <https://www12.senado.leg.br/noticias/materias/2021/05/28/lei-com-penas-mais-duras-contra-crimes-ciberneticos-e-sancionada)>. Access onAugust 19, 2021.

Brotto, GLM *et al.*2017. *Chapter 3 - Victimology and predicting victims of personal violence. The Psychology of Criminal and Antisocial Behavior*,79-144. doi:10.1016/B978-0-12-809287-3.00003-1.

Cavalcante, WF. 2013. *Crimes cibernéticos: noçõesbásicas de investigação e ameaçasna internet*. Revista Jus Navigandi, 3782.Availablein: https://jus.com.br/artigos/25743. Access on: August 22. 2021. ISSN 1518-4862.

Collier B *et al*. 2020. In: *Research Evidence in Policing: Pandemics. The implications of the COVID-19 pandemic for cybercrime policing in Scotland: a rapid review of the evidence and future considerations.*Scottish Institute for Policing Research, 1.

CPS. Technical Report. 2019.Cybercrime - Prosecution Guidance. The Crown Prosecution Service. Available <https://w.ww. cps.gov.uk/legal-guidance/cybercrime-prosecution-guidance. Access onAugust 23, 2021.

Cybersecurity ventures. Relatório Available <https://www. herjavecgroup.com/wp-content/uploads/2018/12/CV-HG-2019-Official-Annual-Cybercrime-Report.pdf>. Access onAugust 23, 2021.

Dahlberg, LL & Krug, EG. 2007.*Violência: um problema global de saúdepública*. Ciência&SaúdeColetiva 11(Sup): 1163-1178.

Fiorillo, Celso AP. Crimes no meioambiente digital e a sociedade da informação. 2. ed. Saraiva, 2016.

Gali, M; Gellert, R.2021. *Data protection law beyond identifiability? atmospheric profiles, nudging and the stratumseind living*. Lab Computer Law & Security Review 40.

Hoepers, C. 2020. *Segurança digital: umaanálise de gestão de riscoemempresas brasileiras*.1: 101-128. Available <https://cetic.br/media/docs/publicacoes/7/20210514123130/estudos-setoriais-seguranca-digital.pdf>. Acesso: 23 ago. 2021. ISBN 978-65-86949-20-9.

Jesus, Damásio de; Milagre, J. A. 2016. Manual de crimes informáticos. Ed. Saraiva.

Lallie, H. S.*et al.*2021. *Cyber security in the age of COVID-19: A timelineandanalysisof cyber-crime and cyber-attacksduringthepandemic*. Computers& Security 105: 102248. doi: 10.1016/j.cose.2021.102248.

Lima, P. M.*et al*. 2020. Confidentialityof cyber-physical systems usingevent-basedcryptography. IFAC PapersOnLine, 53-2: 1735–1740.

LIMA, G. F. 2016. Manual de direito digital: fundamentos, legislação e jurisprudência. Ed. Curitiba: Appris.

LOPES, M. A. 2016. A (indiscreta) história da pornografia.Available <https://super.abril.com.br/historia/a-indiscreta-historia-da-pornografia>. Access on: August 20, 2021.

Malaquias, R. D.2015. Crime cibernético e prova: a investigação criminal embusca da verdade. Ed. Juruá, 2 ed. revista e atualizada. ISBN 978-85-362-5383-1.

Marques, G; Martins, L. 2015. Direito da informática. 2. ed. Coimbra.

Medeiros, FA, Bygrave, LA. 2015. Brazil's Marco Civil da Internet: Does it live up to the hype? Computer Law & Security Review 31: 120-130. doi: 10.1016/j.clsr.

Marra, F. B.2019. Desafios do direitona era da internet: uma breve análisesobreos crimes cibernéticos. Rev. Campo Jurídico, 7 (2):145-167.

Nthala, N.; Flechais, I.2017. *If it's urgent or it is stopping me from doing something, then I might just go straight at it: a study into home data security decisions.* International conference on human aspects of information security, privacy, and trust. Springer: 123-142.

OMS (2002). Available <https://books.google.com.br/books?hl=pt-BR&lr=&id=epuQi1PtY_cC&oi=fnd&pg=PR9&dq=World%25Health%2520+Organization%3B+2002&ots=N4G7eVCdVh&sig=sSwwjRJ8NSA-a8N3hkZupFRDtQM#v=onepage&q=World%25Health%2520%20Organization%3B%202002&f=false>. Accesso: August 23, 2021.

Oliveira, J. R. *et al*. 2021.*Multidimensional sorting framework of cities regarding the concept of sustainable and smart cities with an application to Brazilian capitals.* Sustainable Cities and Society 74 103193. doi:10.1016/j.scs.

Reilly, C. A. 2021. *Reading risk: Preparing students to developcritical digital literacies and advocate for privacy in digital spaces*. Computers and Composition 61: 102652. doi:10.1016/j.compcom.

Reisach, U. 2021. *The responsibilityof social media in times ofsocietalandpoliticalmanipulation.*EuropeanJournalofOperationalResearch 291: 906–917. doi:10.1016/j.ejor.

Rossini, A. E. S. 2009. Breve ensaiosobre a tutelapunitivana Sociedade da Informação, suasesferas de proteção e recentesconquistas. In: Paesani, L. M. O direitonasociedade da Informação. Ed. Atlas v. II: 133-134.

Strupczewski, G. 2021. Defining cyber risk. Safety Science 135: 105143. Doi: 10.1016/j.ssci.

Sydow, S. T. 2015. Crimes informáticos e suasvítimas 2, ed.Saraiva. ISBN: 9788502230552.

Teixeira, T. 2018. Curso de direito e processoeletrônico: doutrina e prática 4. ed. Saraiva.

Urrahman R,Tomar, D. S. 2020. *A new web forensic framework for bot crime investigation. Forensic Science International*. Digital Investigation 33:300943. doi.org/10.1016/j.fsidi.2020.300943.

WHO. 2002. *Reducing risks, promosing healthy*.Health Report.

Yuksel, H., Altunay, Ö. 2020. *Host-to-host TCP/IP connection over serial ports using visible light Communication*. Physical Communication 43: 101222. <https://doi.org/10.1016/j.phycom.>.

****