https://dx.doi.org/10.22161/ijaers.77.3 *ISSN: 2349-6495(P) | 2456-1908(O)*

Criminality and the new information and communication technologies

Marcus Vinicius Campos da Costa[1], Pedro Ivo Oliveira Andrade[2], Rui Machado Júnior[3], Gracinete Franco Antunes[4]

[1]Acadêmico do curso de Direito do Centro Universitário Estácio da Amazônia. Bacharel em Engenharia Elétrica pela Universidade Federal de Roraima. Engenheiro Eletricista da Defensoria Pública do Estado de Roraima, Brazil.
[2]Acadêmico do Curso de Pós-Graduação em Direito Penal e Processo Penal do Centro Universitário Estácio da Amazônia, Mestrando em Segurança Pública, Direitos Humanos e Cidadania (UERR), Bacharel em Direito (Faculdades Cathedral), Bacharel em Engenharia Mecatrônica (UFU), Agente da Polícia Federal, Brazil.
[3]Orientador: Docente do Curso de Graduação e Pós-Graduação em Direito do Centro Universitário Estácio da Amazônia, Mestrando em Segurança Pública, Direitos Humanos e Cidadania (UERR), Especialista em estudos de Criminalidade e Segurança Pública (UFMG), Escrivão da Polícia Federal, Brazil
[4]Coorientadora: Docente do Centro Universitário Estácio da Amazônia, atuando nos cursos de Bacharelado em Direito e Licenciatura em Pedagogia, Brazil

Abstract**—***This work aims to present concepts related to crime in the face of new information and communication technologies. Methodologically, articles and books were used in addition to the legislation dealing with the matter, in particular the Brazilian Penal Code and Law 12.737/12 (Carolina Dieckmann Law). The increasing advance of technology, in addition to providing convenience to people, has expanded the possibility of commitment of crimes. Some already covered by traditional legislation, others needing new classification. In this context, after presenting fundamental notions to understand the topic — such as the concept of computer crime, classification, subjects and applicable legislation —, we sought to analyze some of the main computer crimes, especially the crime of computer device invasion. It was concluded that Criminal Law, in its purpose of protecting the most important legal assets, must act in order to curb the practice of computer crimes. In addition, despite the legislation covering a large part of the crimes committed on the network, the law must continue to update itself in the face of new threats, and the criminal offense of computer device invasion must be improved. Finally, it is addressed the difficulties related to the criminal investigation of this type of crime.*

Keywords ***—Cybercrime, Criminal Law, Law 12.737/12.***

I. INTRODUCTION

Criminal law, as the other branches of law, seeks to keep up with changes in society. However, the challenge of the Law in accompanying them - notably what regards to positivation - has become increasingly difficult, especially in recent decades, due the fast pace that technological development has been taking.

In this scenario, information technology (particularly the internet) brought several conveniences through a large amount of tools and services, such as banking transactions; online shopping (from companies or even between individuals); communication services (WhatsApp, social networks), with the possibility of video calls and conferences; huge possibility of data storage, such as documents, videos, photos, music; transport services (Uber, 99Taxi) and even the legal environment was impacted through judicial process, conference calls, articles, books and video classes distributed online. Anyway, the possibilities are countless, and new tools emerge every day. In fact, we have it all, literally, in the palm of our hands, through the smartphones.

However, this wide range of possibilities also has its negative aspects. The internet stands out as a fertile ground for committing crimes - from crimes already typified, which only use computer devices as a means of practice, to new criminal types. This is due to the increasing spread of access to these technologies, accompanied by the great increase of transactions and communications carried out through the internet, which increases the number of potential victims, as well as the goods that circulate

https://dx.doi.org/10.22161/ijaers.77.3 ISSN: 2349-6495(P) | 2456-1908(O)

because of it, and, consequently, the incentive to commit crimes. Thus, it is up to the State to suppress these conducts, reducing the insecurity of the digital environment.

Due this perspective, this work aims to briefly present the concept and classification of computer crimes and the applicable legislation in Brazil. In addition, an attempt was made to carry out an analysis of some of the most common crimes committed by computer devices, especially the crime of breaching a device. And, finally, address the difficulties encountered in the criminal prosecution of computer crimes, in view of their peculiarities.

II. METHODOLOGY

Several academic publications that address the subject in reference were used to prepare this work: books by renowned jurists to support the main theme of the article, in addition to the legislation dealing with the matter, mainly the Penal Code and Law 12735/12, as well as publications in the press that exemplify the topic addressed.

Thus, the research methodology used in this work was documentary research, since it allows the use of primary sources that provide data and information that have not yet been treated scientifically or analytically, and subject's bibliographic review, with scientific publications consults in periodicals, books, conference proceedings, among other means, in order to better clarify the subject in question, since it typifies crimes of computerized nature, committed through different devices, towards the new information and communication technologies, is not yet a simple task and requires an accurate analysis, precisely because of the lack of similar jurisprudence to clarify this issue. In addition, data and legislation relevant to the topic were also sought.

III. THEORETICAL FRAMEWORK

3.1 The internet andthe Law

A computer network (a term that has become obsolete given the number of new devices that interconnect) is composed of several interconnected computers that exchange information with each other. The internet can then be defined as a network of networks that interconnects billions of devices worldwide. (KUROSE, 2010)

The creation of the internet dates back to the 1960s in the United States, driven by the Cold War, led the country to develop a national communication network aiming to exchange information between different computers. This network would prevent the interruption of the country's chain of command in the event of an attack, in addition, it would prevent the important information concentration on a single machine (NETO, 2010). From there, the internet developed and spread around the world.

In Brazil, the internet originated from the National Research Network Project - RNP -, created in 1989 by MCT (Ministry of Science and Technology), but it was only in 1991 that it began to be disseminated as a national network interconnecting several networks across the country. Furthermore, it was only in 1995 that it was possible to open the Internet to companies and individuals of the Brazilian population, ceasing to be an exclusively academic network (BRASIL, 2016).

Initially, there were beliefs that the internet, due to its decentralized character, could not be regulated by the State, and that there would be absolute freedom in this environment. However, constitutional principles push these beliefs away, bringing the State and the Law to the sphere of information technology, among them: inviolability of intimacy to private life, honor, people's image (art. 5, X, CF), inviolability of communications (art. 5, XII, CF), non-obviation of Judiciary jurisdiction (art. 5, XXXV, CF) (ARAS, 2001).

In addition, despite the functionalities and facilities brought by the internet, it is also an useful tool for illicit acts perpetration – allowing, not only new crimes to be committed but potentialize conventional crimes - because, as João Araújo Monteiro Neto (2003) highlight:

> [...] the existing means for the practice of computer-related crimes are numerous and given the characteristics of these infractions, the traces left are minimal, which makes the repression and the pursuit of these acts an arduous task. (MONTEIRO NETO, 2003, p.43)

It is observed then that the crime's fields also expand with the evolution of society and, therefore, the field of law must also keep up with this evolution, as Vladimir Aras (2001) points out: "if society (or part of it) migrated virtually to cyberspace, there must also go the Law.*Ubisocietas, ibi jus*".

In this context, it is up to the Criminal Law to act, also, in the scope of information technology, taking into account its purpose of protecting the legal assets most valuable to society.

3.2 Computer-related crimes

3.2.1 Concept

The crimes committed by computer devices have different names, among which stands out: computational offenses, information technology crimes, computer crimes,

https://dx.doi.org/10.22161/ijaers.77.3 *ISSN: 2349-6495(P) | 2456-1908(O)*

cybercrimes, electronic crimes, virtual crimes, telematic crimes, information crimes, cyber offenses crimes.

The precise definition of computer crime is not yet consolidated in the doctrine, because of the modernity of this phenomenon. However, in a concise way, it can be said that computer crimes "are all typical, anti-legal and culprit conducts practiced against or with the use of computer systems." (SCHMIDT, 2015).

It is an unquestionable fact that the internet has become part of people's lives, whether through social networks (Instagram, Facebook, Skype, LinkedIn, Twitter, among others), or through applications (apps) or by consulting various sites that aims to make daily life easier, but, at the same time it is used for the positive side, there is also the use on the negative side, such as the installation of a mobile spy application that can hack all data and messages sent or received through WhatsApp, which today is one of the most widely used applications for exchanging messages and communication in audio and video over the internet, for example. In this regard, if any individual takes or receives data without consent and uses it in an improper way, he or she will be committing a crime of this nature.

3.2.2 Classification

Due to its fragmentary character, Criminal Law seeks to suppress only the most serious actions against the most important legal assets, hereof Rogério Greco teaches:

> The legal system is concerned with an infinity of private and collective interests and assets. [...] However, in this legal system**, criminal law has the smallest role regarding the protection of these assets**. It should be noted that by its fragmentary nature, not everything matters to the Criminal Law, but only a small part, a limited portion of assets that are under its protection, but that, undoubtedly, at least in these, **are the most important and necessary for the relief of society** (GRECO, 2017, p. 140 emphasis added)

By using a computer device, the criminal faces several possibilities for committing crimes, in other words, to violate fundamentally important legal assets. These assets may already be protected by traditional Criminal Law, or not, due to the lack of specific legislation.

According to the offended legal asset, the cybercrime may be classified as proper or improper. Thus, improper cybercrime occurs when the computer is used only as a mean to execute a common crime, producing naturalistic results, threatening or damaging legal assets other than information technology (ARAS, 2001). Thereby, the computer is not essential for the crime's perpetration, which could be practiced even without its help, it is the case of fraud, theft through fraud (embezzlement of bank account money, payment of bills by credit card improperly), crimes against honor, possession of child pornography, etc.

In the other hand, for the proper computer crimes, the computer is essential for the practice of the crime, considering that the legal object protected by these crimes is the computer system itself, the security of these systems and their data, for example (SCHMIDT, 2015). Examples are: invasion of a computer device (art. 154-A of the CP), insertion of false data in the public administration information system (art. 313-A of the CP).

3.2.3 Active and Passive Subjects

When it comes to computer crimes, the active subject that first comes to most people's minds is the mythical hacker - an expert in the operation of computers and computer systems, who uses his skills to invade those systems. However, João Araújo Monteiro Neto (2003) highlights that:

> One time previously the profile of the cybercriminal was this. Currently, with the facilities caused by the development of Softwares and Hardware, as well as the innumerable information available on the network about the subject, any individual who has the minimum notions of how to operate a computer can be considered a potential computer criminal. (MONTEIRO NETO, 2003, p.41)

The wide spread of communication technologies, such as smartphones, computers and tablets, guarantees access to millions of people in services such as SMS, e-mails and instant messages, because of that, the number of potential victims today is huge. In this scenario, criminals can use social engineering[1] to mislead people and gain advantages for themselves, without the need of advanced technical knowledge.

Furthermore, regarding the large number of today's social networks users, added to the feeling of anonymity and impunity that the internet brings, everyone has the potential to commit crimes against honor, for example.

[1]"Social engineering is a popular way for cybercriminals to discover users' personal information - such as passwords or bank details - without having to exploit security breaches in systems. In general, the strategy is hacking users, not their devices, in order to convince them that they are giving information to trusted people or services. The tactics used include e-mail messages and fake pages or psychological tricks to distract victims" (KURTZ, 2016)

https://dx.doi.org/10.22161/ijaers.77.3 *ISSN: 2349-6495(P) | 2456-1908(O)*

Finally, given the wide range of computer crimes, any person - physical or legal - can be a victim of one of these crimes, if this person has, for example, his assets misappropriated, his property damaged or his information breached (ALMEIDA, MENDOÇA, *et al.*, 2015)

3.3Brazilianlegislation

The Legality Principle, a major advance in criminal law, is enshrined in art. 5, XXXIX, of the Federal Constitution: "there will be no crime without a previous law that defines it, nor a penalty without prior legal agreement." In this circumstance, in spite of the criminals' use of new communication technologies, a large part of the crimes committed using these technologies are already typified in the Penal Code of 1940, thus classified as improper cybercrimes.

> For the Judiciary, 95% of the crimes committed electronically are already typified in the Brazilian Penal Code because they characterize common crimes practiced through the internet. The other 5%, for which there would be no legal framework, cover transgressions that only exist in the virtual world, such as the distribution of electronic viruses and DDoS[2] attacks. (CASSANTI, 2014, p. 24 APUD FILGUEIRAS, et al., 2015, p.3)

It is not, it should be noted, legislative gaps being filled by analogy - since Brazilian criminal law does not allow the use of this integration technique in malam partem, due to the principle of legality (GRECO, 2017b) –, but an innovation while committing the crime. On this point, the understanding of STF Minister SepúlvedaPertence, in HC:

> "Computer Crime": child sex scene publication (ECA, art. 241), through insertion in a BBS / Internet network of computers, attributed to minors: typicality: expert evidence necessary to demonstrate authorship: HC partially accepted. [...] 2. It is not the case, therefore, to fill a gap in the incriminating law by analogy: once it is understood the typical decision of the criminal conduct, the technical means employed to carry it out may even be of a later invention to the edition of the penal law: **the invention of gunpowder did not demand redefinition of homicide to make explicit the death given to others by means of a firearm is a homicide.** (STF, 1998 emphasis added)

Regarding proper computer crimes, the two main laws that regulate the subject, in the criminal sphere, are laws 12,735 / 2012 and 12,737 / 2012. (BORTOT, 2017). The first changed item II of §3 °, of art. 20 of Law 7.716 / 1989, which “defines crimes resulting from prejudice of race or color”.

Art. 20 of the law has as its type “to practice, induce or incite discrimination or prejudice of race, color, ethnicity, religion or national origin”. The combination of paragraphs 2nd and 3rd, of article 20, establishes that if any of the crimes established in the caput is committed through the media or publication of any nature, the judge may determine, according to item II, of § 3rd, “the cessation of the respective radio, television or eletronic transmission or publication by any means”. The part of the provision item II, which allows the judge to determine the cessation of electronic broadcasts or publication by any means, is a law innovation, since the previous type only foresaw the radio and television broadcasts, without making reference to electronic broadcasts. In other words, the amendment came “to allow a request for the removal of discriminatory content to be made by the Judge, not only on radio, TV or the Internet, but in any possible way.” (BORTOT, 2017, p. 350)

Beyond that, Law 12.735/2012 determined, in art. 4th, that the judicial police must create structures, sectors and teams specialized in combating computer crimes.

IV. ANALYSIS AND RESULTS

4.1 Most common computer crimes

Taking into consideration all the theory presented, a brief analysis of some of the most common computer crimes is carried out. Among them, we highlight the fraud (art. 171, CP) and theft qualified by fraud (art. 155, §4, II, CP), which despite being similar are not the same. In both, the criminal uses fraud - cunning, insidious means, in order to make the victim incur or be kept in error (GRECO, 2017a) - to obtain an illicit advantage. However, in the first one, the victim, induced in error, voluntarily disposes of his assets, while in the second one, fraud is used to evade the victim's surveillance, while the perpetrator subtracts his assets without his knowledge (DE OLIVEIRA JÚNIOR, 2015). They are classified as improper computer crimes.

2 O DDoS (*Distributed Denial of Service*) is a type of virtual attack, in which “the master computer enslaves several machines and makes them access a given resource on a given server all at the same time. Thus, all zombies access together and uninterruptedly the same resource as a server. Taking into account that web servers have a limited number of users that can be served at the same time, this large number of traffic makes it impossible for the server to be able to fulfill any request. The server can restart or even hang depending on the resource that was victimized ” (CANALTECH).

https://dx.doi.org/10.22161/ijaers.77.3 *ISSN: 2349-6495(P) | 2456-1908(O)*

Examples of these crimes are abundant and widely reported in the press, such as sending SMS, e-mails, WhatsApp messages posing as banks, cell phone operators or other institutions, in order to obtain information (names, CPFs, passwords, security codes) in order to obtain financial benefits (embezzling money from a bank account, for example) or even requesting cash deposits from third parties, posing as the victim.

It is noteworthy that during the pandemic times the internet use became much more intense with many people performing frequent banking operations, working remotely, and also shopping, making all their data available on the network, and with more people using the internet, more virtual crimes were committed and many users, either through misinformation or through identical/cloned applications, or due to the persuasion on the part of criminals, end up being victims of these crimes, which have already been carried out previously. It is evident that offenders take advantage of the pandemic itself, a period of vulnerability of the population, in order to convince the victims, as is happening in many cities in the country where, data are requested by people who pass themselves off as Ministry of Health officials to apply frauds by telephone.

In this manner, recently, a practice that has been alerted by the press is WhatsApp hijacking. The crime can occur in several ways: posing as an employee of an institution and then requesting the WhatsApp access code directly from the victim (NOGUEIRA, 2020); through SIM Swap[3]; or by QRLjacking[4]. After gaining access to the victim's WhatsApp, the fraudster starts to send messages to his contacts requesting loans from the victim's friends and family who, because they trust him, end up making bank deposits in the agent's account, as happened with the nutritionist JanaínaGoston who was the victim of virtual scam, as reported by the news.

[3] "[...] consists of transferring the phone line to a SIM chip other than the one on your cell phone. It can be done in some ways that almost always involve social engineering: criminals pretend to be the victim and, with their personal information, get the operator to activate the phone number elsewhere." (JUNQUEIRA, 2020).

[4] "[...] technique capable of cloning QR codes to capture the credentials of the user who wants to login. The hacker just needs to convince the target to use his own cell phone to scan the cloned image on a fake website. When the strategy is successful, the criminal gains access to the victim's complete conversation history without arousing suspicion" (ALVES, 2019).

Another crime that he found on the Internet and other technologies as a means of dissemination and storage is child pornography, typified in Article 241-A and 241-B of the Child and Adolescent Statute (ECA).

> Art. 241-A. Offer, exchange, make available, transmit, distribute, publish or disseminate by any means, including by means of a computer or telematics system, photography, video or other record containing explicit sex scene or pornographic sex scene involving a child or adolescent:
>
> Penalty - imprisonment, from 3 (three) to 6 (six) years, and a fine.
>
> Art. 241-B. Acquire, own or store, by any means, photography, video or other form of record that contains explicit sex scene or pornographic sex scene involving a child or adolescent:
>
> Penalty - imprisonment, from 1 (one) to 4 (four) years, and a fine.

Analyzing the criminal types, it is possible to infer that the legislator decided to criminalize both the agent who distributes child pornography and the agent who acquires or even stores it, the second one, however, incurs into a lesser penalty. It should be noted that this crime can be committed by any means, and is therefore classified as an improper cybercrime.

Finally, as previously mentioned, Law 12.737/12 (Carolina Dieckmann Law), innovated Brazilian legislation by creating the criminal type of computer device invasion, inserting art. 154-A in the Penal Code, a proper cybercrime, considering that the legal object protected is the third party's computer device, with the consequent protection of its data and information.

> Art. 154-A. Invade someone else's computer device, connected or not to the computer network, through an undue violation of a security mechanism and with the purpose of obtaining, tampering or destroying data or information without the express or tacit authorization of the device owner or installing vulnerabilities to obtain an illicit advantage:
>
> Penalty - imprisonment, from 3 (three) months to 1 (one) year, and a fine.
>
> § 1º The same penalty applies to those who produce, offer, distribute, sell or broadcast a device or computer program in order to allow the practice of the conduct defined in the caput.
>
> § 2º The penalty is increased from one sixth to one third if economic damage results from the invasion.

https://dx.doi.org/10.22161/ijaers.77.3 *ISSN: 2349-6495(P) | 2456-1908(O)*

§ 3º If the invasion results in obtaining content from private electronic communications, trade or industrial secrets, confidential information, as defined by law, or the unauthorized remote control of the invaded device:

Penalty - imprisonment, from 6 (six) months to 2 (two) years, and a fine, if the conduct does not constitute a more serious crime.

§ 4º In the case of § 3, the penalty is increased by one to two thirds if there is disclosure, commercialization or transmission to third parties, in any capacity, of the data or information obtained.

§ 5º The penalty is increased from one third to half if the crime is committed against:

I - President of the Republic, governors and mayors;

II - President of the Supreme Federal Court;

III - President of the Chamber of Deputies, the Federal Senate, the State Legislative Assembly, the Legislative Chamber of the Federal District or the City Council; or

IV - top manager of the direct and indirect federal, state, municipal or Federal District administration.

The aforementioned penal type requires the following elements: a) the invasion; b) someone else's computer device; c) connected or not to the computer network; d) through an undue violation of the security mechanism; e) for the purpose of obtaining, tampering with or destroying data or information without the express or tacit authorization of the holder of the device; f) or install vulnerabilities to obtain an illicit advantage (GRECO, 2017a).

It should be noted that for the crime to occur the object under protection (computer device) cannot belong to the author. "So, for example, if someone puts information on someone else's computer and the owner of the device is accessing the data inserted there, the offense under study will not be characterized" (GRECO, 2017a, p.765).

In addition, it does not matter whether the device is connected to a computer network or not - like the internet, for example. In other words, if someone, realizing that a friend forgot his computer at this person's home and he or she decide to invade it, if other elements of the type were present, the crime of 154-A will be perpetrated (GRECO, 2017a).

However, there is still a criticism to be made to the text of the Law. As it constitutes an element of the type, the need for the conduct to occur through an undue violation of the security mechanism, in case that there is an improper entry into another device, but without the breach of any security device (login and password, for example), the conduct cannot be considered typical.

It is not uncommon that people avoid place access passwords, for example, on their computers, allowing anyone who has access to them to access their data. However, even without the existence of a password, no one is allowed to break into another's computer, unless the owner expressly or tacitly gives permission. However, for purposes of typical configuration, regarding the requirement contained in the penal type under analysis, there will only be a criminal infraction if there is an undue violation of the security mechanism by the invading agent. (GRECO, 2017a, p.766 emphasis added)

Finally, the agent's conduct must be carried out in order to obtain, tamper with or destroy data or information without the express or tacit authorization of the device owner or to install vulnerabilities to obtain an illicit advantage. Therefore,

[...] it is not the simple invasion, by itself, through the undue violation of the security mechanism that matters in the practice of the criminal offense [...] but, it must have a special purpose, that is, what called special purpose of action, which consists of obtaining, tampering or destroying data or information without the express or tacit authorization of the device owner. (GRECO, 2017a, p. 766)

Anyone can be an active subject of this crime, with the exception of the owner of the computer device. Meanwhile, the victim will be the owner of the hacked device, or anyone else who has data or information stored at that device. (GRECO, 2017a)

It is essential to point out that the penalty imposed is from three (3) months to one (1) year of detention, and a fine. The qualified modality, under the terms of §3º, increases the penalty for imprisonment, from six (6) months to two (2) years. There are also special causes that increase the sentence defined in §§2º, 4º and 5º. As so, the jurisdiction for the judgment of this crime lies with the Special Criminal Court, except in cases when the application of the qualifier and special causes that increase penalty causes the maximum penalty exceed the limit of two (2) years, under the terms of art. 61, of Law 9.099/95. Besides, it is possible to apply the conditional suspension of the process, pursuant to art. 89 of the same legislative diploma. In this context, it is important to note that the crime of invading a computer device is considered a less offensive potential crime.

https://dx.doi.org/10.22161/ijaers.77.3 *ISSN: 2349-6495(P) | 2456-1908(O)*

4.2 Computer crimes´ criminal investigation

Finally, it is essential to highlight the difficulties encountered in investigating computer crimes, which are diverse. Unlike other crimes, in computer crimes it is not possible to identify the agent visually or through documents, often the criminal uses false identification, or, as pointed out above, is impersonating other people. Furthermore, evidence of the materiality of the crime is extremely volatile and can be easily erased or lost (SCHMIDT, 2015).

This way, criminal prosecution in this type of crime requires specialized expertise to demonstrate the materiality and authorship of the crime and as pointed out by Schmidt (2015): "Often, for the proper materiality verification, it is necessary to intercept the flow communications carried out through a computer".

Beyond that, data recorded by internet service providers or application providers (such as social networks, e-mails and instant messaging programs, hosting providers) is essential to provide the IP address, date and time of access to its services, referring to the moment of the crime, which will only be provided by court order (SHIMABUKURO, 2017). The combination of the three data is necessary when requesting information from the connection provider, in order to identify where a certain illegal conduct arose, considering that the IP is dynamically allocated - to each computer access to the internet, a new IP is assigned to it (SCHMIDT, 2015).

It is important to point out that this procedure should be carried out as soon as possible, based on the criminal action identification, because despite the Marco Civil da Internet turning mandatory for providers to keep this information, highlights Adriana Shimabukuro (2017):

> Decree No. 8.771/2016, which regulated the Marco Civil da Internet Law, determines that connection and application providers must delete user data as soon as the retention period ends. Considering that the deadlines are short, 6 (six) months for application providers and 1 (one) year for connection providers, the authorities now have another challenge to comply with the law.

After identifying the criminal action origin's place, the next step is to comply with search and seizure warrants issued by the competent courts, aiming to collect computer devices in general, including hard drives, memory cards and flash drives, in order to search for digital traces, materiality and authorship evidence of the crimes. For that, dedicated tools are used for this purpose, as added by Márcio Rodrigo de Freitas Carneiro (2017): "The complete and detailed storage media processing requires dedicated tools that normally take considerable time [...]".

Among the main functions performed by these tools, we highlight: a process that alert the presence of known files or to ignore common system files; files categorization based mainly in the common formats used; text indexing extracted from file types; thumbnails provision and video frames selection to speed up responses and analysis; system's deleted files recovery; explicit image detection, implemented to categorize possible images, including pornography, to aid child pornography exams (CARNEIRO, 2017).

It should be noted, however, that when the device seized is a smartphone, there are extra difficulties:

> a) Commonly, passwords are used to block the device, which by default automatically lock after a short time not using the equipment. There are many models that make it impossible to access data without a password and there are no known breaking methods.
>
> [...]
>
> b) Access to internal storage media is not simple and straightforward as with computers and notebooks. Cell phones' internal Flash memories are soldered to the device's printed circuit, and all access is limited through the USB communication port. (CARNEIRO, 2017 p. 51).

Finally, as explained above, this whole process starts from the agent's IP identification, however it is possible to hide or even change this identifier through tools such as proxies and services such as TOR (The Onion Router) (SHIMABUKURO, 2017). Adriana Shimabukuro (2017, p. 25) states that this last tool can "use up to 3 (three) fake addresses in different countries, making tracking almost impossible."

TOR is one software used to access the Dark Web or Darknet, which is a closed network, used to share content anonymously, composed of non-indexed data, in other words, it cannot be detected by search engines like Google or Bing (SHIMABUKURO, 2017).

Having this in mind, the difficulties of investigating these crimes remains evident, since the authorities still encounter several obstacles to effectively perform their functions.

V. CONCLUSION

The evolution and dissemination of communication and information technologies brought ease and convenience to people due the large number of tools and services

https://dx.doi.org/10.22161/ijaers.77.3 *ISSN: 2349-6495(P) | 2456-1908(O)*

available. However, considering the neutrality of these technologies, it is also used as a tool for committing and enhancing crimes.

So, as seen, it is a Criminal Law function - in the constitutional and penal principles' view, such as the jurisdiction unfeasibility and fragmentation – to protect the legal assets most dear to society, wherever it may be, whether in the physical or virtual world.

In this regard, traditional criminal law already covers a large part of crimes committed at the Internet, given that many of them are common crimes with new execution means. It is important to have in mind, always, that it is not a case of using analogy in the classification of these crimes, which is emphatically prohibited by criminal principles. In the other hand, others criminal facts lack their own typification, as a result of having been created along with technological innovation.

As an example of these crimes, we highlight fraud, qualified theft through fraud, child pornography and the computer device invasion. It is noteworthy that this last crime is a recent creation in the Penal Code, considered a pure cybercrime. And, although it deserves applause for its innovation, there are criticisms against this new penal type because it demands that the conduct must occur through an undue violation of the security mechanism, which ends up weakening it, for leaving other harmful conducts outside the criminal law's scope.

Finally, it should be noted that harmful conducts, such as DDoS attacks and virus's distribution, still exists and are not covered by the current legislation, and deserve a legislator analysis in order to seek for protection over the legal assets guarded by the Criminal Law. In addition, it is mandatory to increase the investments in the investigative area related to these crimes, given the difficulty and the need for technical training, for the criminal prosecution of this crime's type.

REFERENCES

[1] Almeida, D. J. et al. Crimes Cibernéticos. Cadernos de graduação ciências humanas e sociais, Aracaju, SE, n. 3, Março 2015. 215-236.

[2] Alves, P. QRLjacking: entenda o sequestro de contas do WhatsApp pelo QR Code. Techtudo, 2019. Disponivel em: <https://www.techtudo.com.br/noticias/2019/06/qrljacking-entenda-o-sequestro-de-contas-do-whatsapp-pelo-qr-code.ghtml>. Acesso em: 30 Abril 2020.

[3] Aras, V. Crimes de informática. Uma nova criminalidade. Jus, 2001. Disponivel em: <https://jus.com.br/artigos/2250/crimes-de-informatica>. Acesso em: 30 Abril 2020.

[4] Bortot, J. F. Crimes cibernéticos: aspectos legislativos e implicações na persecução penal com base nas legislações brasileira e internacional. VirtuaJus, Belo Horizonte, v. 2, n. 2, 2017. 338-362.

[5] Brasil. Decreto-Lei nº 2.848, de 7 de dezembro de 1940. Código Penal. Disponivel em: <http://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm>. Acesso em: 30 Abril 2020.

[6] Brasil. Lei nº 12.735, de 30 de novembro de 2012. Altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal, o Decreto-Lei nº 1.001, de 21 de outubro de 1969 - Código Penal Militar, e a Lei nº 7.716, de 5 de janeiro de 1989, para tipificar condutas r. Disponivel em: <http://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2012/Lei/L12735.htm>. Acesso em: 30 Abril 2020.

[7] Brasil. Lei nº 12.737, de 30 de novembro de 2012. Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal; e dá outras providências. Disponivel em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm>. Acesso em: 30 Abril 2020.

[8] Brasil. Lei nº 8.069, de 13 de julho de 1990. Dispõe sobre o Estatuto da Criança e do Adolescente e dá outras providências. Disponivel em: <http://www.planalto.gov.br/ccivil_03/leis/l8069.htm>. Acesso em: 30 Abril 2020.

[9] Brasil. Lei nº 9.099, de 26 de Setembro de 1995. Dispõe sobre os Juizados Especiais Cíveis e Criminais e dá outras providências, Brasília, DF. Disponivel em: <http://www.planalto.gov.br/ccivil_03/leis/l9099.htm>. Acesso em: 30 Abril 2020.

[10] Brasil. Câmara dos Deputados. Comissão parlamentar de inquérito destinada a investigar a prática de crimes cibernéticos e seus efeitos deletérios perante a economia e a sociedade neste país. Relatório final. Brasilia, p. 263. 2016.

[11] Canaltech. O que é DoS e DDoS? Canaltech. Disponivel em: <https://canaltech.com.br/produtos/o-que-e-dos-e-ddos/>. Acesso em: 02 Maio 2020.

[12] Carneiro, M. R. D. F. Perícia de informática nos crimes cibernéticos. Investigação e prova nos crimes cibernéticos, São Paulo, n. 1, p. 33-54, 2017.

[13] De Oliveira Júnior. Furto mediante fraude ou estelionato? Migalhas, 2015. Disponivel em: <https://www.migalhas.com.br/depeso/227115/furto-mediante-fraude-ou-estelionato>. Acesso em: 30 Abril 2020.

[14] Filgueiras, A. W. N. et al. Crimes virtuais: ameaças reais. in Evidosol/Ciltec-Online. Anais eletrônicos, Belo Horizonte, 2015. Disponivel em: http://www.periodicos.letras.ufmg.br/index.php/anais_linguagem_tecnologia/article/view/12109.

[15] Greco, R. Código Penal: comentado. 11ª. ed. Niterói/RJ: Impetus, 2017a.

[16] Greco, R. Curso de Direito Penal: parte geral. 19ª. ed. Niterói/RJ: Impetus, v. I, 2017b.

[17] Junqueira, D. WhatsApp invadido? Saiba como funciona o golpe SIM Swap. Olhar Digital, 2020. Disponivel em: <https://olhardigital.com.br/dicas_e_tutoriais/noticia/sim-

https://dx.doi.org/10.22161/ijaers.77.3 *ISSN: 2349-6495(P) | 2456-1908(O)*

swap-saiba-como-criminosos-sequestram-as-contas-de-whatsapp/79348>. Acesso em: 30 Abril 2020.

[18] Kurose, J. F. Redes de computadores e a Internet: uma abordagem top-down. 5ª. ed. São Paulo: Pearson, 2010.

[19] Kurtz, J. O que é engenharia social. Techtudo, 2016. Disponivel em: <https://www.techtudo.com.br/dicas-e-tutoriais/noticia/2016/11/o-que-e-engenharia-social.html>. Acesso em: 30 Abril 2020.

[20] Monteiro Neto, J. A. Crimes informáticos uma abordagem dinâmica ao direito penal informático. Pensar - Revista de Ciências Jurídicas, Fortaleza/CE, n. 8, Fevereiro 2003. 39-54.

[21] Nogueira, M. Como caí no golpe que sequestra a conta do WhatsApp para extorquir dinheiro dos contatos. Folha de S. Paulo, 2020. Disponivel em: <https://www1.folha.uol.com.br/cotidiano/2020/01/como-cai-no-golpe-que-sequestra-a-conta-do-whatsapp-para-extorquir-dinheiro-dos-contatos-telefonicos.shtml>. Acesso em: 30 Abril 2020.

[22] Schmidt, G. Crimes Cibernéticos. Jusbrasil, 2015. Disponivel em: <https://gschmidtadv.jusbrasil.com.br/artigos/149726370/crimes-ciberneticos>. Acesso em: 30 Abril 2020.

[23] Shimabukuro, A. Cibercrime: quando a tecnologia é aliada da lei. Investigação e prova nos crimes cibernéticos, São Paulo, n. 1, p. 17-32, 2017.

[24] STF. Habeas Corpus: HC 76689, Relator(a): Min. Sepúlveda Pertence. DJ 06-11-1998. STF, 1998. Disponivel em: <http://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=AC&docID=76856>. Acesso em: 30 Abril 2020.